

# Configuration Manual

MSc Research Project  
MSc Cyber Security

Ankit Kantilal Patel  
Student ID: X21101850

School of Computing  
National College of Ireland

Supervisor: Prof. Jawad Salahuddin

**National College of Ireland**  
**MSc Project Submission Sheet**



**School of Computing**

**Student Name:** Ankit Kantilal Patel  
**Student ID:** x21101850  
**Programme:** MSc Cyber Security **Year:** 2022  
MSc Research Project  
**Module:** Jawad Salahuddin  
**Lecturer:**  
**Submission Due Date:** 15th December 2022  
**Project Title:** Detecting Malicious URL using Extreme Learning Machine Algorithm  
**Word Count:** 678 **Page Count:** 7

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:** Ankit Kantilal Patel  
**Date:** 14th December 2022

**PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST**

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
<b>Attach a Moodle submission receipt of the online project submission,</b> to each project (including multiple copies).	<input type="checkbox"/>
<b>You must ensure that you retain a HARD COPY of the project,</b> both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

<b>Office Use Only</b>	
Signature:	
Date:	
Penalty Applied (if applicable):	

# Configuration Manual

Ankit Kantilal Patel  
Student ID: x21101850

## 1 Introduction

The manual documents about all the necessary tools and the technologies required to implement the research model. The manual is further divided into various sections. Section 2 mentions about the environment setup required, Section 3 mentions about the tools and software's used, Section 4 mentions about implementing the project, and in the last references are mentioned.

## 2 Environment Setup

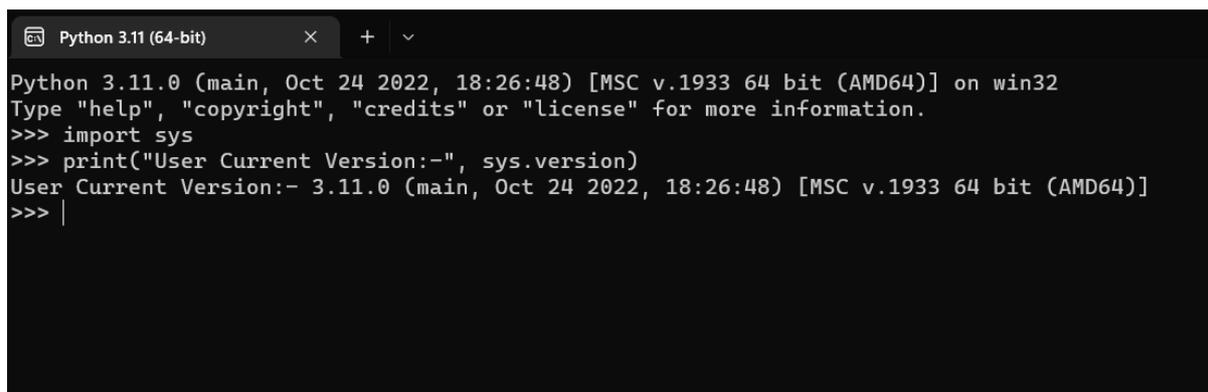
Below mentioned configuration was used to implement the model.

- Processor: Intel i7
- Memory: 16GB RAM
- Programming language: Python3
- Python Environment: Jupyter Notebook, Anaconda Navigator

## 3 Tools and Software Used

Below mentioned software were used to implement the model.

- For programming Language, we have used python 3.11.0.



```
Python 3.11 (64-bit) × + ▾
Python 3.11.0 (main, Oct 24 2022, 18:26:48) [MSC v.1933 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import sys
>>> print("User Current Version:-", sys.version)
User Current Version:- 3.11.0 (main, Oct 24 2022, 18:26:48) [MSC v.1933 64 bit (AMD64)]
>>> |
```

Figure 1. Python Version

- For dataset processing and performing operations on it, we have used a python open source project called jupyter. It uses python kernel for processing and performing operations on the datasets.

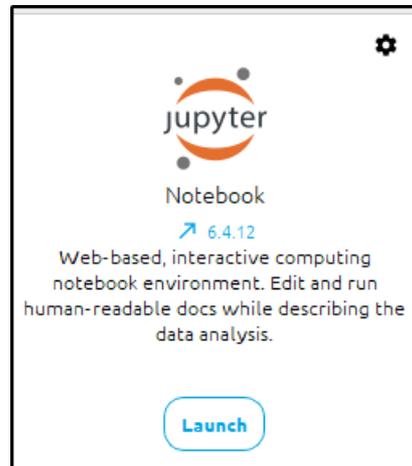


Figure 2. Python Jupyter

## 4 Implementation of the Model

**Step 1 :-** We have used anaconda navigator, to use python jupyter notebook. First, we need to install an anaconda navigator. Anaconda Navigator [1] can be installed from the website mentioned in the reference. We launch the navigator, and we can see jupyter in the main dashboard then we click on launch to launch jupyter notebook as shown in below Figure 3.

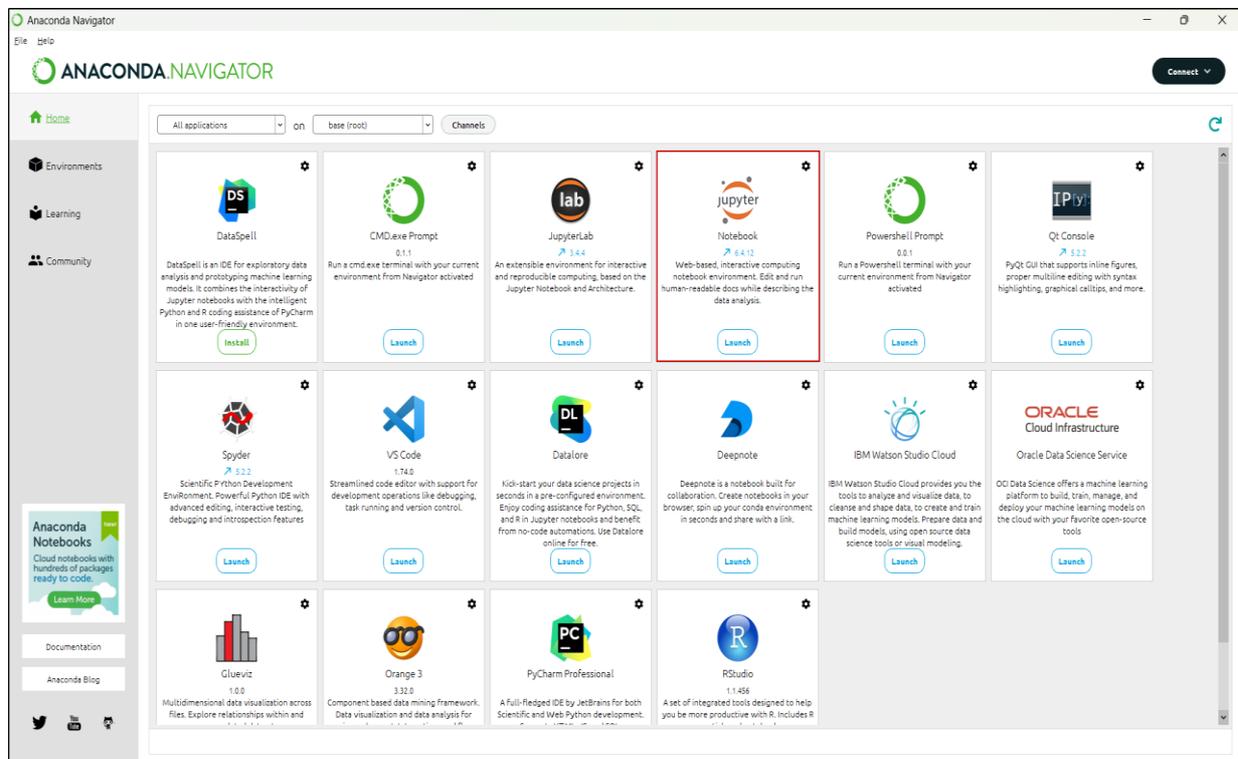
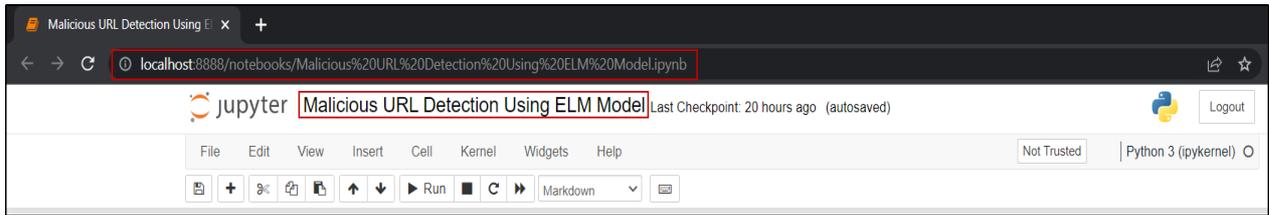


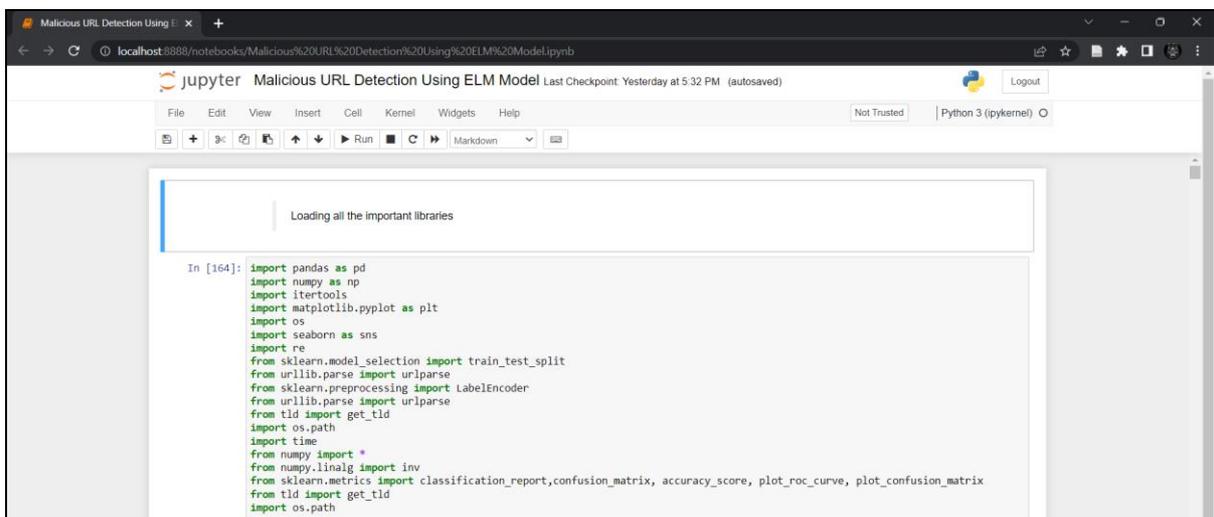
Figure 3. Anaconda Navigator

**Step 2 :-** Open the file “Malicious URL Detection Using ELM Model.ipynb” in the jupyter notebook.



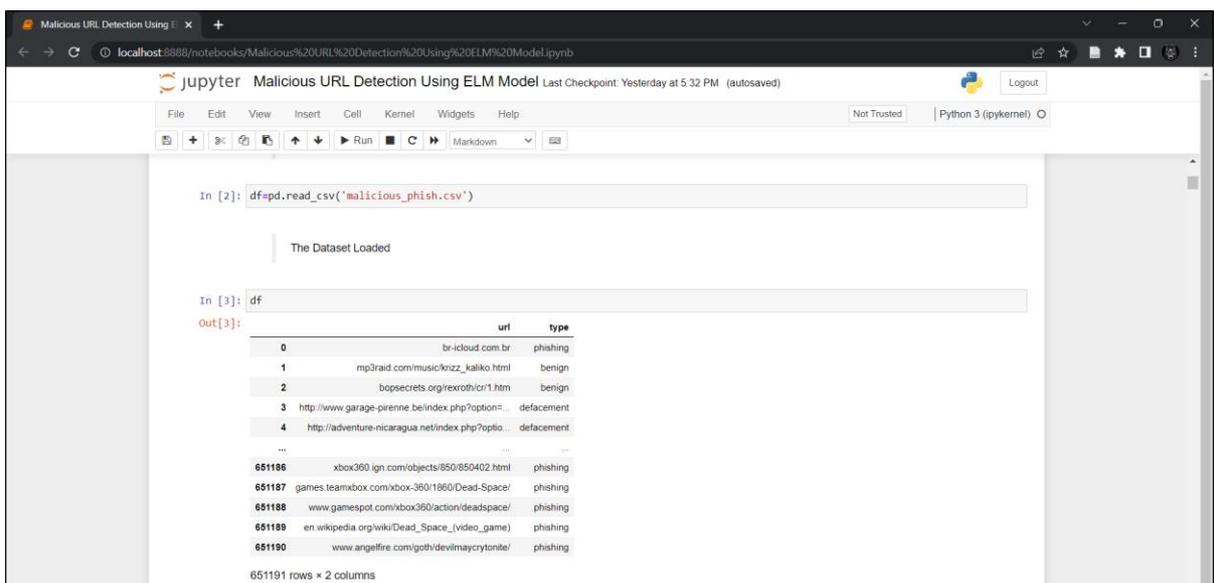
**Figure 4. Ipynb file launched in Jupyter**

**Step 3 :-** From here we start the implementation of the model, we start by importing all the necessary libraries for the model.



**Figure 5. Libraries Imported for the Model**

**Step 4 :-** We load the dataset [2] using pandas libraries.



**Figure 6. Loading the Dataset in the Model**

### Step 5 :- Features extracted from the dataset.

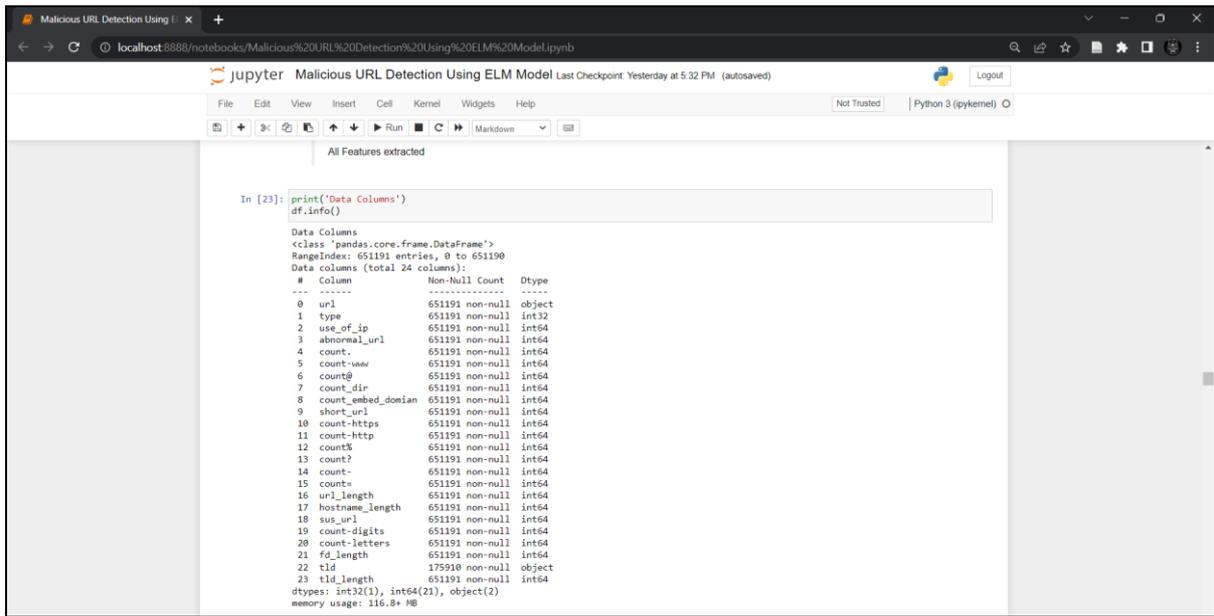


Figure 7. Dataset Features Extracted

### Step 6 :- Enter URLs in the urls array to be detected as malicious and the model detects it.



Figure 8. Final Detection of URL

### Step 7 :- Code in Jupyter can be executed by using Run button.

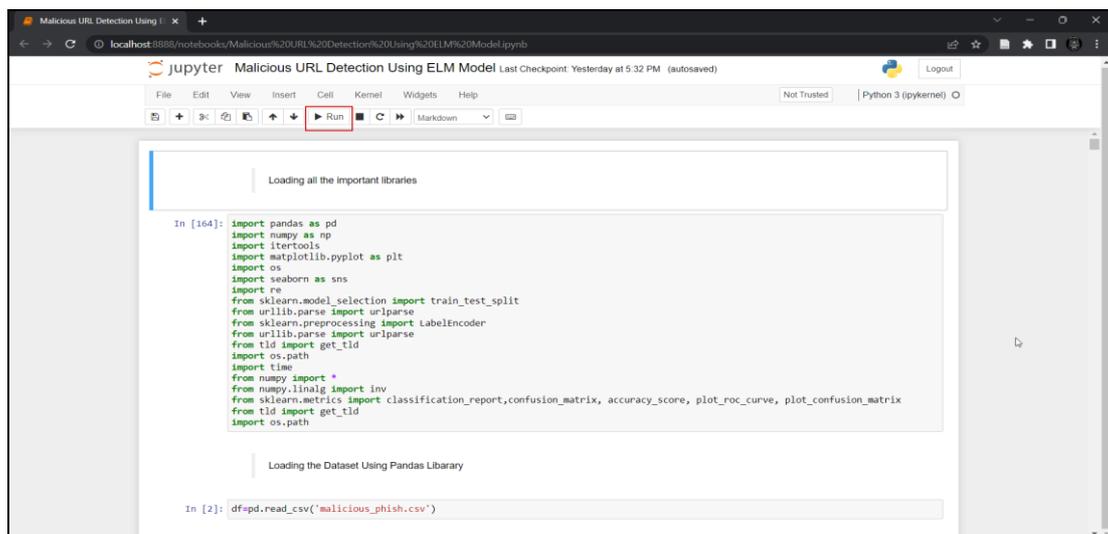


Figure 9. Code Execution in Jupyter

## References

- [1] “Anaconda | Anaconda Distribution,” Anaconda. <https://www.anaconda.com/products/distribution> (accessed Dec. 13, 2022).
- Feng, G. and Buyya, R. (2016). Maximum revenue-oriented resource allocation in cloud, *IJGUC* 7(1): 12–21.
- [2] “Malicious URLs dataset.” <https://www.kaggle.com/datasets/sid321axn/malicious-urls-dataset> (accessed Dec. 06, 2022).