National College of Ireland

Configuration Manual

MSc Research Project

MSc Cloud Computing

Sandeep Kumar Mylavarapu

Student ID: 23204346

School of Computing

National College of Ireland

Supervisor: Rejwanul Haque

National College of Ireland
MSc Project Submission Sheet
School of Computing

Student Name:	SANDEEP KUMAR MYLAVARAPU
Student ID:	23204346
Programme	MSc CLOUD COMPUTING **Year:** 2025
Module:	RESEARCH PROJECT
Lecturer:	REJWANUL HAQUE
Submission Due Date:	29-01-2025
Project Title:	ANALYSING THE EFFECTIVENESS OF MACHINE LEARNING ALGORITHMS IN INTRUSION DETECTION SYSTEM FOR IOT NETWORKS
Word Count:	**1271 Approx**

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: SANDEEP KUMAR MYLAVARAPU

Date: 29-01-2025

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

SANDEEP KUMAR MYLAVARAPU
Student ID: 23204346

1 Introduction

This configuration manual is going to give the most detailed description of how to install, configure and to use throughout the "Analysing the effectiveness of Machine Learning Algorithms in Intrusion Detection Systems for Iot Networks" project. The focus of the project is to implement and to develop different machine learning techniques and to compare how effectively they perform intrusion detection from the network traffic.These mainly consist of the accuracy, precision, recall, and F1 score among others.

2 System Requirements

"Analysing the effectiveness of Machine Learning Algorithms in Intrusion Detection Systems for Iot Networks" requires the following system specifications:

2.1 Hardware Requirements

Operating System:Windows 11 or macOS, or Linux (Ubuntu 20.04 or newer recommended)
Processor: Intel Core i5 or higher (or equivalent for non-Intel processors)
System Type: 64-bit Operating System
RAM: 8GB (16GB recommended for large datasets)
Hard Disk Space: 500GB or more (SSD preferred for faster data processing)
Display: 1920x1080 resolution (higher resolution preferred for better UI/UX)
Graphics Card: Optional(NVIDIA GPU recommended for accelerated training with TensorFlow or PyTorch)

2.2 Software Requirements

Anaconda: Python environment manager: Version 3.8 or higher
Jupyter Notebook: Version 6.0.3 or higher is required to run as well as visualize experiments.
Python: It is preferable to use a library with Python 3.8 or higher this is the version of the language used in the library stable version 3.8 or higher.

3 Installation

Step 1: Install Python and Required Libraries

I make sure that Python 3.8 or above is installed on my system. Then, I open a terminal or command prompt and run the following command to install the required libraries:

- pandas and numpy for the purpose of data manipulation and numerical operations.
- scipy for scientific computations.
- sklearn for machine learning tools, including splitting data, preprocessing, and training classifiers.
- matplotlib and seaborn for data visualization.
- warnings for handling and suppressing warning messages.

Step 2: Download the Project Files

I download the Performance Analysis of Machine Learning Algorithms in Intrusion Detection Systems project zip file from the repository. After downloading I extract the files to a folder on my computer.

Step 3: Open the Python File

In the Jupyter Notebook interface, I locate the "ANALYSING THE EFFECTIVENESS OF MACHINE LEARNING ALGORITHMS IN INTRUSION DETECTION SYSTEM FOR IOT
NETWORKS.ipynb" file and open it by clicking on it.

Step 4: Run the Notebook

I run the cells in the notebook sequentially by selecting a cell and pressing Shift + Enter. The notebook will automatically load the dataset, preprocess it, split it into training and test sets, and apply various machine learning algorithms such as:

- ***Random Forest Classifier ● Support Vector Classifier (SVC) ● K-Nearest Neighbors (KNN)***

It will also compute performance metrics like accuracy, precision, recall, and F1-score.

Step 5: View the Results

Once I run the notebook, I can view the following evaluation metrics for the models:

- Accuracy
- Precision
- Recall
- F1 Score

Additionally, I can see a confusion matrix and a classification report that summarizes the model's performance.

4 Configuration

No further modifications are possible for the notebook named Analysing the effectiveness of Machine Learning Algorithms in Intrusion Detection Systems for Iot Networks. The dependency of these functionalities can be found in the installation instructions provided above.

5 Troubleshooting

If I encounter any issues while running Analysing the effectiveness of Machine Learning Algorithms in Intrusion Detection Systems notebook for Iot Networks, I can follow these troubleshooting steps:

1. If I encounter any issues while running the Analysing the effectiveness of Machine Learning Algorithms in the Intrusion Detection Systems for Iot Networks notebook, I can follow these troubleshooting steps:
2. Missing Libraries: In case I receive a message saying that a certain library is missing I could verify that I have compiled all the dependencies.

3. Jupyter Notebook Not Opening: If it doesn't open, I verify if the environment I am working in is activated (in case I am using it) and whether there is competition for the ports Jupyter occupies.
4. Model Performance Issues: If the model is not well performing, I make sure the data set is properly uploaded and analyzed. I look for cases in the data where values may be missing out of the ordinary or contain an error. Of course, there is further preprocessing: I can normalize or scale the features; or split the data for training/testing in a different manner.
5. Memory Issues: In the case the analysis is very large and reaching the memory limit or being time-consuming I can always try decreasing the data or running the data analysis in a system with ample space.
6. Confusion Matrix or Report Errors: If there is an error when creating confusion matrix or class report, I check if the models have been trained appropriately and the forecast labels with the output labels.

6 Conclusion

This document presents the complete instructions on how to install, configure and use the Performance Analysis of Machine Learning Algorithms in Intrusion Detection Systems notebook and I follow them to the letter. Python with the accompanying tools including Scikit-learn, TensorFlow, and Keras offers a sound platform on which to train, test the models needed to identify intrusions in network traffic.It allows me to input data and try to guess what algorithm will perform better Random Forest, SVC or KNN and then gives me metrics such as accuracy, precision, recall and F1 score to compare them.Leveraging these results when developing enhancements or better deployment strategies for intrusion detection system models will be useful.To ease the process of installation and use in case of any hardship the user is taken through a troubleshooting section in case of any installation difficulties or problems encountered during the execution process. There is no need for further setup of the notebook apart from installing the dependencies provided, and all the tools are provided to assess whether the models accurately catch network intrusions.

References

https://jupyter.org/
https://www.python.org/downloads/release/python-3810/