National College of Ireland

Configuration Manual

MSc Internship Cyber Security

Hanok Vijay Chukka
Student ID: x19128622

School of Computing National College of Ireland

Supervisor: Imran Khan

National College of Ireland Project

Submission Sheet School of Computing

Student Name:	Hanok Vijay Chukka
Student ID:	x19128622
Programme:	Cyber Security
Year:	2019
Module:	MSc Internship
Supervisor:	Imran Khan
Submission Due Date:	28/09/2020
Project Title:	Configuration Manual
Word Count:	919
Page Count:	9

I here by 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 there leant 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 there port template. To use other author's written or electronic work is illegal(plagiarism) and may result in disciplinary action.

Signature:	Hanok Vijay chukka
Date:	26th September 2020

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	Q
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	Q
You must ensure that you retain a HARDCOPY 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.	Q

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

Hanok Vijay Chukka
x19128622

1 Introduction

This configuration manual provides the details of the proposed work and model used for detecting malware using machine learning algorithms like Multinomial Naïve Bayes (NB), Support Vector Machine (SVM) and Random Forest (RF).The proposed system extracts feature from. APK files and training is given for supervised learning. Different ML models like Multinomial Naïve Bayes, Random Forest and SVM are used as prediction models. With these ML techniques a framework is realized to have provision for protection of malware in Android devices or applications. The proposed solution continues giving support with increased quality. The review of literature [1], [2], [3], [4], [5] showed the utility of the machine learning algorithms.

2 System Configuration

This section provides an overview of the system used for the implementation of this model.

Hardware Specification

This project is developed using a laptop running Windows 10 operating system. The system specifications are as shown in Figure 1.

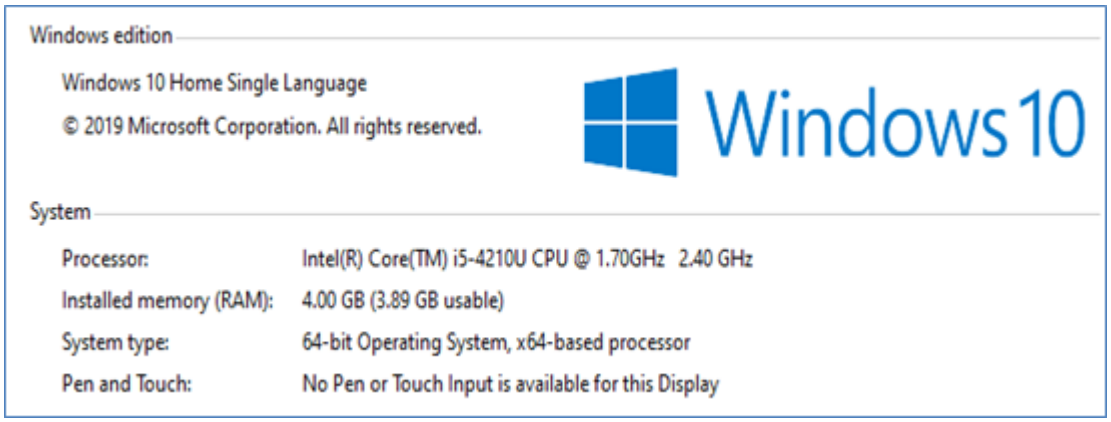

Figure 1: Hardware specification of system with Windows 10 OS

3 Software Specification

This section describes details of the tools and technologies used while developing the project.

Tool	Version	Description
Python Language[1]	3.6	It is used to implement the project.
Spyder[2]	3	It is the IDE used to implement the project coding.

Table 1: Tools used in this model

[1] https://www.anaconda.com/

[2] https://www.anaconda.com/

4 Working

This section illustrates step by step procedure used for setting up the proposed model and demonstrates itsworking.

SoftwareInstallation

Python anaconda is installed that supports both Python language and also Syper IDE.

https://www.anaconda.com/

Implementation

After installing Anaconda

1. Open Anaconda
2. Open Spyder IDE
3. Open all source files of the project.
4. Run main.py

To run the project:

1. Spyder IDE
2. File → Open →Go to folder where source code is → choose all .py files to open.

Execution of Detection Models

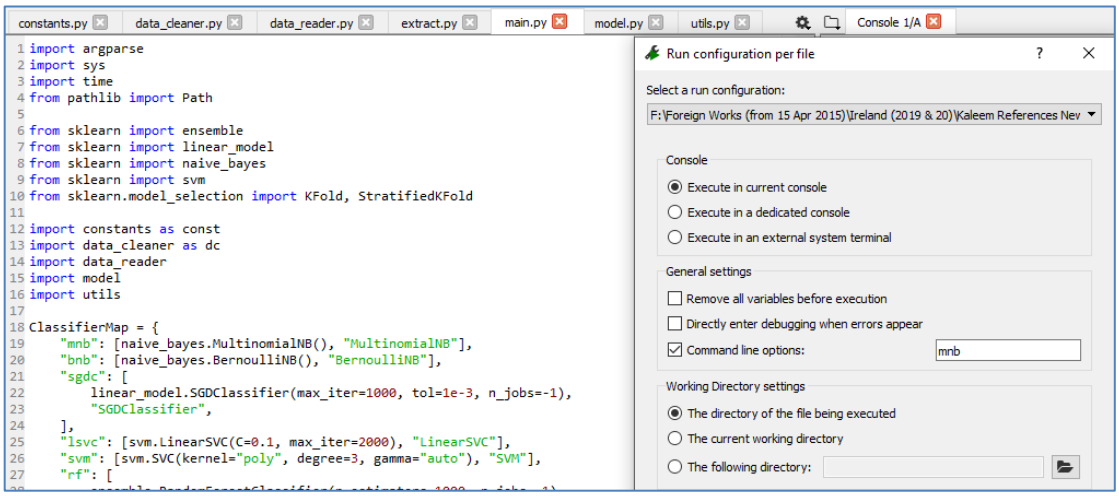

Figure 2: Execution of Android malware detection system with Multinomial Naïve Bayes model

As presented in Figure 2, the execution of the Android malware prediction model is made with

command line argument “mnb”. Based on the argument, the ClassifierMap function in invoked and corresponding model is applied to the dataset in order to achieve Android malware detection.

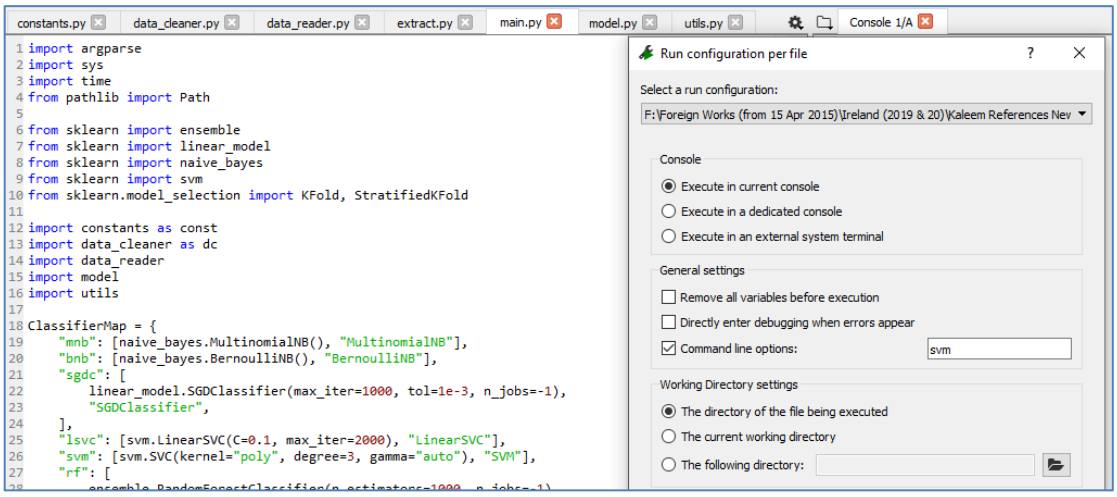

Figure 3: Execution of Android malware detection system with SVM model

As presented in Figure 3, the execution of the Android malware prediction model is made with command line argument “svm”. Based on the argument, the ClassifierMap function in invoked and corresponding model is applied to the dataset in order to achieve Android malware detection.

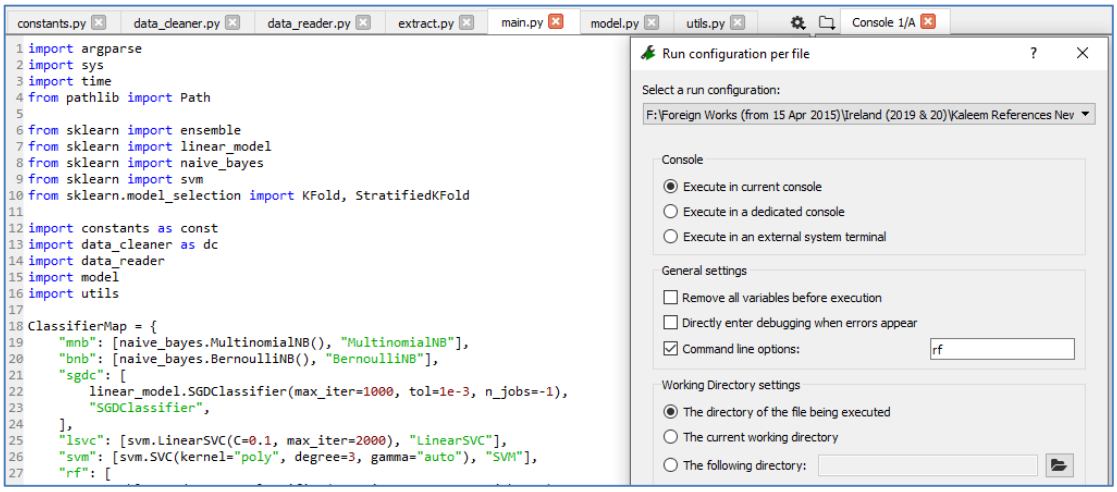

Figure 4: Execution of Android malware detection system with RF model

As presented in Figure 4, the execution of the Android malware prediction model is made with command line argument “rf”. Based on the argument, the ClassifierMap function in invoked and corresponding model is applied to the dataset in order to achieve Android malware detection.

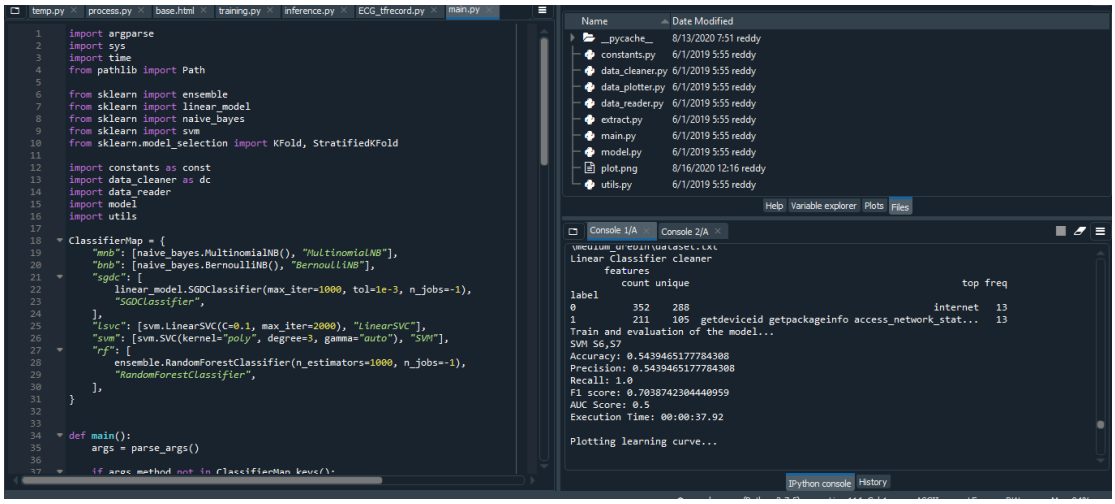

Figure 5: Result of SVM execution

As shown in Figure 5, SVM execution results are shown.

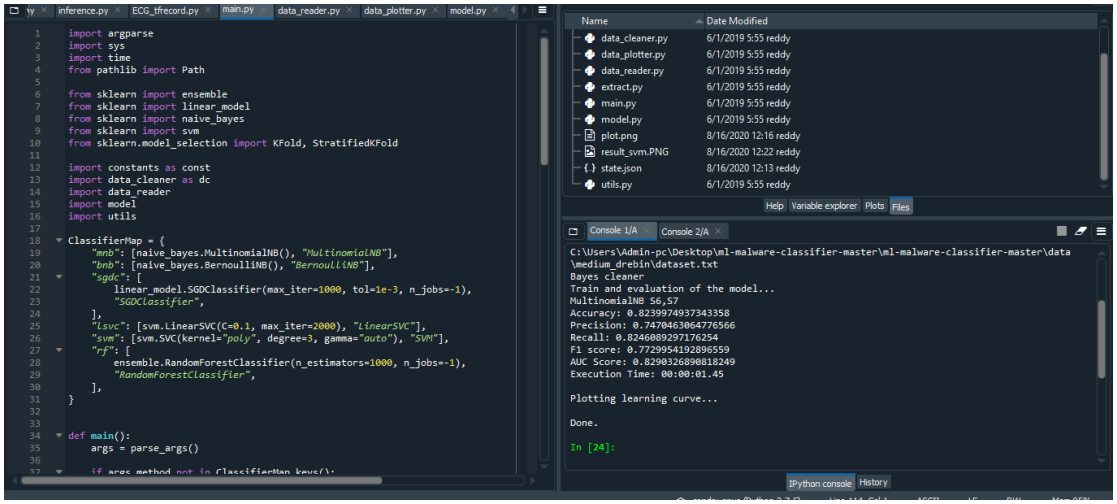

Figure 6: Results of Multinomial NB

As shown in Figure 6, Multinomial NB execution results are shown.

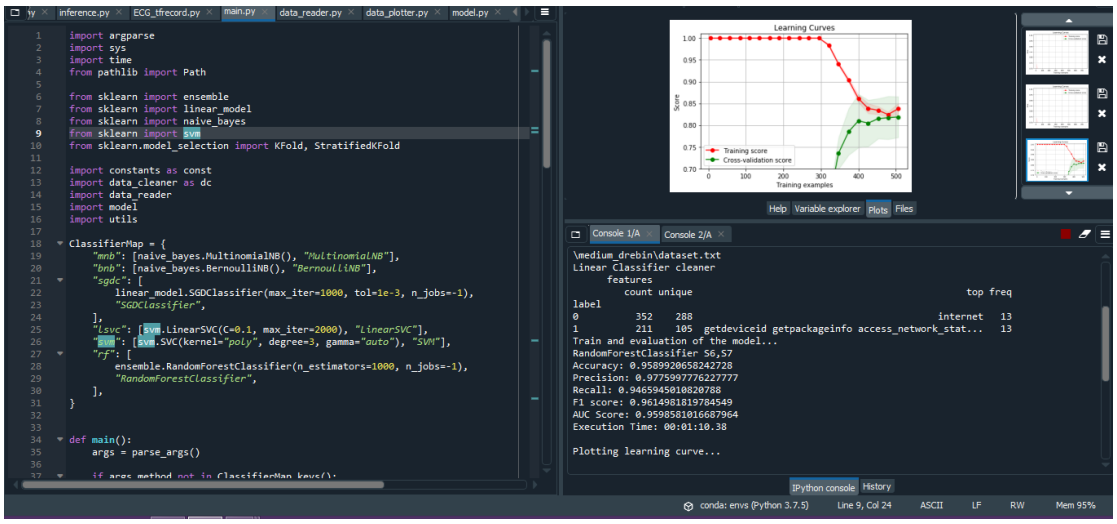

Figure 7: Results of RF

As shown in Figure 7, RF execution results are shown.

5 References

[1] Anwar, S., Zain, J. M., Inayat, Z., Haq, R. U., Karim, A., & Jabir, A. N. (2016). A static approach towards mobile botnet detection. 2016 3rd International Conference on Electronic Design (ICED) p1-5

[2] Hatcher, W. G., & Yu, W. (2018). A Survey of Deep Learning: Platforms, Applications and Emerging Research Trends. IEEE Access, 6, p24411–24432

[3] Hasan, R., Zawoad, S., & Haque, M. M. (2016). StuxMob: A situational-aware malware for targeted attack on smart mobile devices. MILCOM 2016 - 2016 IEEE Military Communications Conference p1-6

[4] Han, Q., Liang, S., & Zhang, H. (2015). Mobile cloud sensing, big data, and 5G networks make an intelligent and smart world. IEEE Network, 29(2),p 40–45

[5] Malatras, A., Freyssinet, E., & Beslay, L. (2015). Mobile Botnets Taxonomy and Challenges. 2015 European Intelligence and Security Informatics Conference p1-4