Report On

Mobile Botnet Detection

Submitted in partial fulfillment of the requirements of the Mini project in Semester VI of Third Year Artificial Intelligence & Data Science

by

Yash Patil (Roll No. 18)
Shubhamkar Patra (Roll No. 35)
Chetan Sapkal (Roll No. 37)

Mentor
Prof. Sneha Yadav

University of Mumbai

Vidyavardhini's College of Engineering & Technology

Department of Artificial Intelligence & Data Science

(A.Y. 2022-23)

Vidyavardhini's College of Engineering & Technology

Department of Artificial Intelligence & Data Science

CERTIFICATE

This is to certify that the Mini Project entitled **“Mobile Botnet Detection”** is a bonafide work of **Yash Patil (Roll No. 18), Chetan Sapkal (Roll No. 37) and Shubhamkar Patra (Roll No. 35),** submitted to the University of Mumbai in partial fulfilment of the requirement for the award of the degree of **“Bachelor of Engineering”** in Semester VI of Third Year **“Artificial Intelligence & Data Science” .**

Ms. Sneha Yadav
Mentor

Ms. Sejal D’mello Deputy-HOD	Dr. Vikas Gupta Head of Department	Dr. H.V. Vankudre Principal

Vidyavardhini's College of Engineering & Technology

Department of Artificial Intelligence & Data Science

Mini Project Approval

This Mini Project entitled "**Mobile Botnet Detection" Yash Patil (Roll No. 18), Chetan Sapkal (Roll No. 37) and Shubhamkar Patra (Roll No. 35)** is approved for the degree of **Bachelor of Engineering** in in Semester VI of Third Year **Artificial Intelligence & Data Science.**

Examiners

` `

1………………………………………
(Internal Examiner Name & Sign)

2…………………………………………
(External Examiner name & Sign)

Date:
Place:

Abstract

Android, being the most widespread mobile operating systems is increasingly becoming a target for malware. Malicious apps designed to turn mobile devices into bots that may form part of a larger botnet have become quite common, thus posing a serious threat. This calls for more effective methods to detect botnets on the Android platform. Hence, in this paper, we present a deep learning approach for Android botnet detection based on Convolutional Neural Networks (CNN). Our proposed botnet detection system is implemented as a CNN-based model that is trained on 342 static app features to distinguish between botnet apps and normal apps.

Acknowledgement

We would like to express our sincere gratitude to our advisor Sneha Yadav for the continuous support of our study and research, for her patience, motivation, enthusiasm, and immense knowledge. His guidance helped us in all the time of research and writing of this thesis. We could not have imagined having a better advisor and mentor for our study.

Contents

Abstract **i**

Acknowledgments **ii**

1 Introduction **1**

1.1 Introduction

1.2 Problem Statement & Objectives **2**

1.3 Scope **3**

2 Literature Survey

2.1 Survey of Existing System/**SRS** **4**

2.2 Limitation Existing system or Research gap **5**

2.3 Mini Project Contribution **5**

3 Proposed System (e.g. New Approach of Data Summarization)

3.1 Architecture/ Framework/Block diagram **6**

3.2 Algorithm and Process Design **7**

3.3 Details of Hardware & Software **8**

3.4 Results for Validation and Verification **9**

3.5 Conclusion and Future work. **12**

3.6 Plagiarism Report **14**

3.7 Code **15**

References **18**

Introduction

1.1 Introduction:

Smart technologies are used by developers and smartphone users rapidly in use these days. By using this technology, the threat is getting infected with malicious viruses like botnets. These viruses mainly attack android apps. Some of the types of the famous types of attacks on theandroid app are increasing these days. The flow of this malware is to command and control the app's server. This mobile botnet runs automatically when it gets installed in the systemwithout the antivirus. Mobile botnet obtains overall access to device change himself continuously. The overall methodology for the detection and prevention of mobile botnets isproposed in this paper. For testing against the apps, the ISCX dataset is used to detect the botnet-infected apps.

A botnet consists of a number of Internet-connected devices under the control of a malicious user or group of users known as botmaster(s). It also consists of a Command and Control (CC) infrastructure that enables the bots to receive commands, get updates and send status information to the malicious actors. Since smartphones and other mobile devices are typically used to connect to online services and are rarely switched off, they provide a rich source of candidates for operating botnets. Thus, the term ‘mobile botnet’ refers to a group of compromised smartphones and other mobile devices that are remotely controlled by botmasters using CC channels.

The overall system is built using python andMachine Learning models like SVM. Some python libraries are used in this system like Pandas, NumPy, Sci-Kit, Seaborn, etc.

1.2 Problem Statement:

Problem Statement:

In this project we Detect Botnet App. Botnet App means some malware are installed in the App through the mobile. That time loss your Important Mobile Data. So we avoid all the loss. Our proposed botnet detection system is implemented as a CNN-based model that is trained on app features to distinguish between botnet apps and normal apps.

.

1.3 Aim & Objectives

Aim:

They have a strong ability to detect security threats, to collect malware signatures and to understand the motivation and technique behind the threat.

Objective:

The goal is to set the user up for being unknowingly exposed to a malware infection. You'll commonly see hackers exploit security issues in software or websites or deliver the malware through emails and other online messages

Literature Survey

2.1 Survey of Existing System:

1.Paper Name:Cooperative Network Behaviour Analysis Model for Mobile Botnet Detection
Author: Meisam Eslahi, Moslem Yousefi
Abstract ::-— Recently, the mobile devices are well integrated with Internet and widely used by normal users and organizations which employ Bring Your Own Device technology. On the other hand, the mobile devices are less protected in comparison to computers. Therefore, the mobile devices and networks have now become attractive targets for attackers. Amongst several types of mobile threats, the mobile HTTP Botnets can be considered as one of the most sophisticated attacks. A HTTP Bots stealthily infect mobile devices and periodically communicate with their controller called Botmaster. Although the Bots hide their activities amongst the normal web flows, their periodic pattern has been used as a measure to detect their activities. In this paper we propose a cooperative network behaviour analysis model to identify the level of periodicity posed by mobile Bots. Finally three metrics is proposed to detect Mobile HTTP Botnets based on similarity and correlation of their group activities. Test results show that the propose model can efficiently classify communication patterns into several periodicity categories and detect mobile Botnet.

2.Paper Name:- Mobile Botnet Detection: A Deep Learning Approach Using Convolutional Neural Networks
Author: Mohammed K. Alzaylaee
Abstract : — Android, being the most widespread mobile operating systems is increasingly becoming a target for malware. Malicious apps designed to turn mobile devices into bots that may form part of a larger botnet have become quite common, thus posing a serious threat. This calls for more effective methods to detect botnets on the Android platform. Hence, in this paper, we present a deep learning approach for Android botnet detection based on Convolutional Neural Networks (CNN). Our proposed botnet detection system is implemented as a CNN-based model that is trained on 342 static app features to distinguish between botnet apps and normal apps. The trained botnet detection model was evaluated on a set of 6,802 real applications containing 1,929 botnets from the publicly available ISCX botnet dataset. The results show that our CNN-based approach had the highest overall prediction accuracy compared to other popular machine learning classifiers. Furthermore, the performance results observed from our model were better than those reported in previous studies on machine learning based Android botnet detection.

3.Paper Name: Detection of Mobile Botnets using Neural Networks
Author: Milan Oulehla, David Malanik
Abstract : This poster deals with botnets, the most dangerous kind of mobile malware, and their detection using neural networks. Unlike common mobile malware, botnets often have a complicated pattern of behaviour because they are not managed by predictable algorithms but they are controlled by humans via command and control servers (CC servers) or via peer-to-peer networks. However, they have certain common features which have been revealed by analysis of contemporary mobile botnets. These features have been used for creation of a neural network training set. Finally, the design of parallel architecture using neural network for useful detection of mobile botnets has been described.

4.Paper Name: Mobile Botnet Detection: A Deep Learning Approach Using Convolutional Neural Networks
Author: Suleiman Y. Yerima, Mohammed K. Alzaylaee
Abstract: — Android, being the most widespread mobile operating systems is increasingly becoming a target for malware. Malicious apps designed to turn mobile devices into bots that may form part of a larger botnet have become quite common, thus posing a serious threat. This calls for more effective methods to detect botnets on the Android platform. Hence, in this paper, we present a deep learning approach for Android botnet detection based on Convolutional Neural Networks (CNN). Our proposed botnet detection system is implemented as a CNN-based model that is trained on 342 static app features to distinguish between botnet apps and normal apps. The trained botnet detection model was evaluated on a set of 6,802 real applications containing 1,929 botnets from the publicly available ISCX botnet dataset. The results show that our CNN-based approach had the highest overall prediction accuracy compared to other popular machine learning classifiers. Furthermore, the performance results observed from our model were better than those reported in previous studies on machine learning based Android botnet detection.

5. Paper Name: Toward a Detection Framework for Android Botnet
Author: Wadi' Hijawi, Hossam Faris
Abstract: —Android is one of the most popular and widespread operating systems for smartphones. It has several millions of applications that are published at either official or unofficial stores. Botnet applications are kind of malware that can be published using these stores and downloaded by the victims on their smartphones. In this paper, we propose Android botnet detection method based a new set of discriminating features extracted based from the analysis of Android permissions (i.e. Protection levels for all available Android permissions). Then we compared the prediction power of different machine learning models before and after adding these features to the state-of-art requested permissions features in Android. We used four popular ML classifiers (i.e. Random Forest, Multilayer Perceptron neural networks, Decision trees, and Naive Bayes) for our experiments and we found that the new set of features have a tiny improvement on the performance in the case of decision trees and Random forest classifiers

2.2 Limitation Existing system or Research gap:

Mobile botnets are a significant threat to mobile devices and networks. While there have been various approaches proposed for detecting mobile botnets, there are still some limitations and research gaps that exist.
Some of the limitations of existing mobile botnet detection systems include:

i. Limited detection accuracy: Mobile botnet detection systems can sometimes generate false positives or false negatives, which can limit their effectiveness in accurately identifying botnet activity.

ii. Inability to detect new botnets: Most mobile botnet detection systems are signature-based and rely on known botnet signatures. However, new botnets may not have known signatures, making it difficult for detection systems to identify them.

iii. Performance overhead: Mobile botnet detection systems may require significant computational resources, leading to performance overhead and potential battery drain on mobile devices.

iv. Privacy preservation: Mobile botnet detection systems may require access to sensitive user data, raising concerns about privacy. More research is needed to develop detection systems that can preserve user privacy while still detecting botnet activity effectively.

2.3 Mini Project Contribution

Botnet Detection is an important problem in cybersecurity, as botnets can be used to launch a variety of attacks, including Distributed Denial of Service(DDoS), spamming, and phishing attacks. There are Several approaches to detecting botnets, including network-based detection, host-based detection.
Here is a mini project contribution for botnet detection using machine learning.

Proposed System

3.1 Framework/Block Diagram

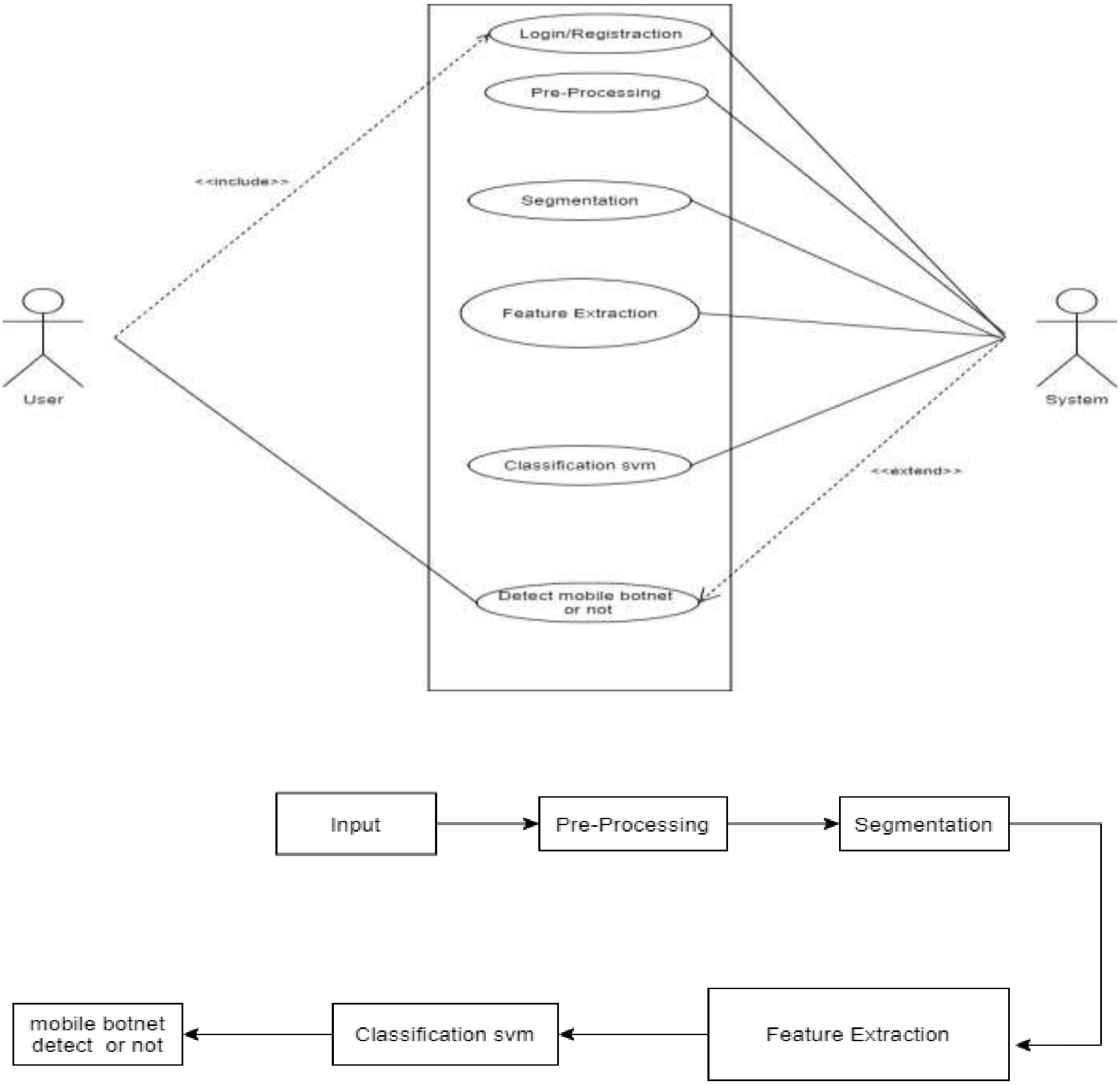


Figure 3.1: Block Diagram of the Application

3.2 Working:

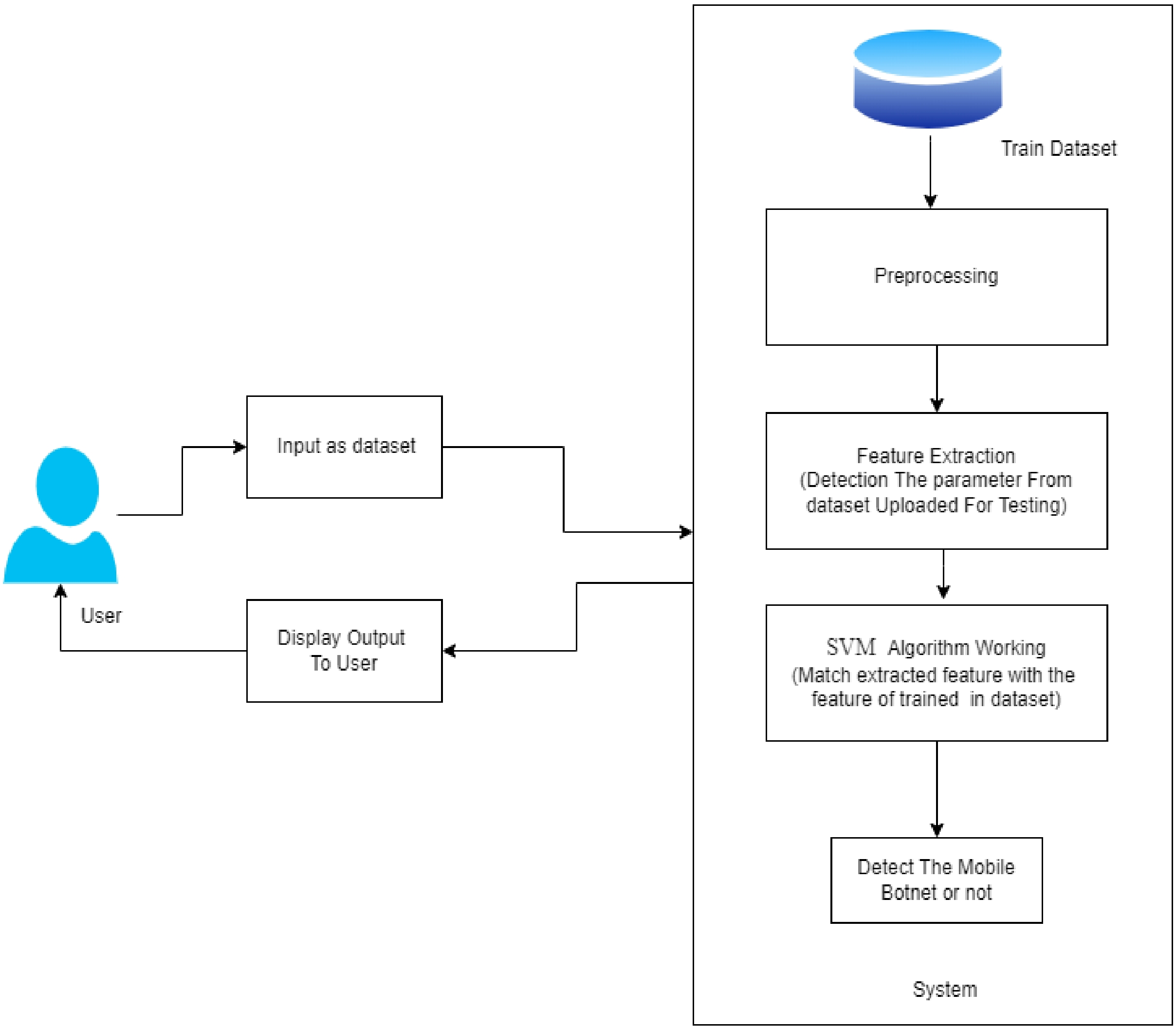

Train Dataset
Preprocessing
Feature Extraction (Detection The parameter From dataset Uploaded For Testing)
SVM Algorithm Working (Match extracted feature with the feature of trained in dataset)
Detect The Mobile Botnet or not
System
Input as dataset
User
Display Output To User

Figure 3.2: Working of the Application

3.3 Details of Hardware & Software

Software requirements for Development:

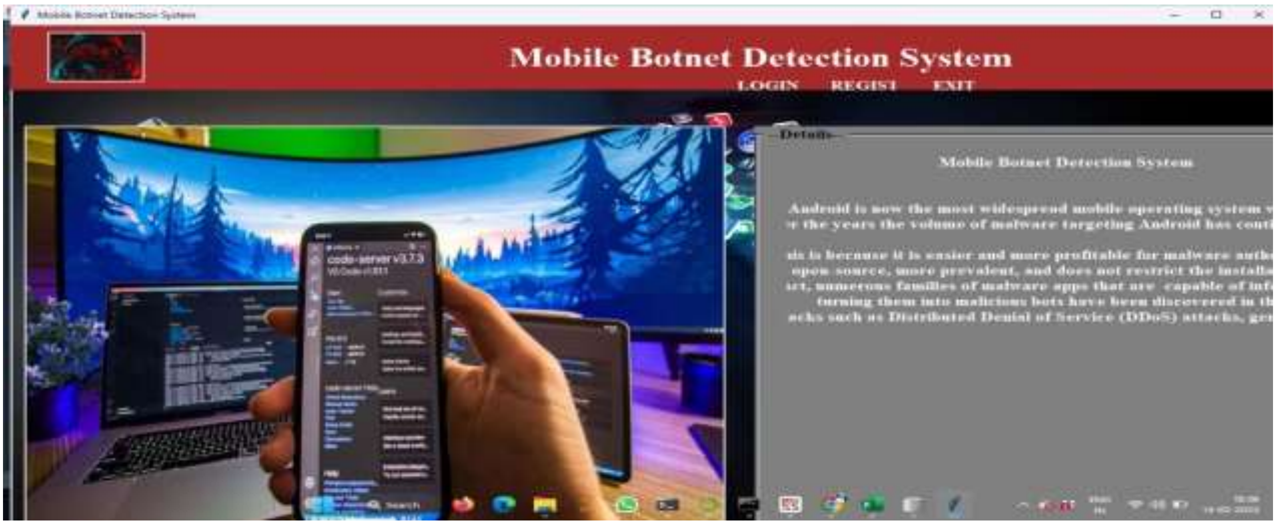
- ➢ Operating System: 64-bit Microsoft Windows 8/10
- ➢ Processor : Intel i5 Processor
- ➢ IDE : Spyder or Pycharm
- ➢ Programming Language : Python

Hardware requirements for Development:

- ➢ RAM: 8 GB or more
- ➢ Disk Space: 40 GB of available disk space minimum (Data Set of CT Scan images is to be used hence minimum 40 GB Hard Disk memory is required)
- ➢ CPU Architecture: x86_64 CPU architecture
- ➢ Nvidia Graphic Processor for better training time

3.4 Results and Discussion

Output:

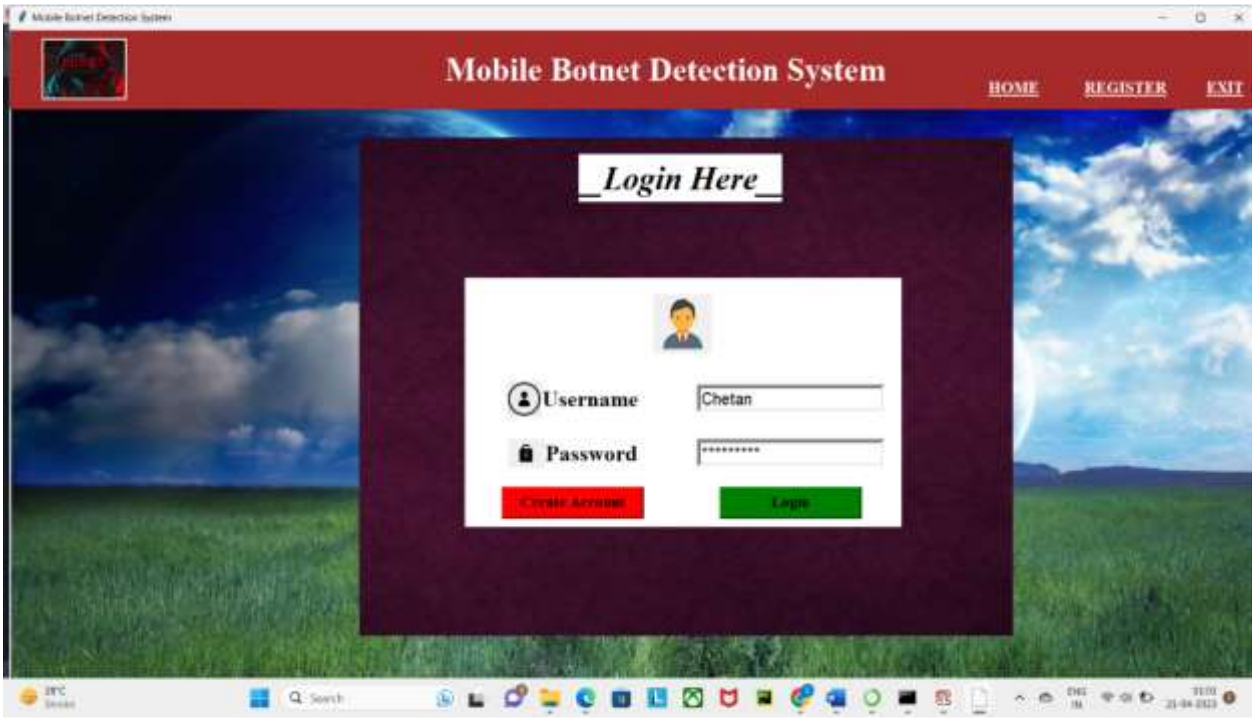

Mobile Botnet Detection System
Mobile Botnet Detection System
LOGIN
REGIST
EXIT
Details

Mobile Botnet Detection System

Android is now the most widespread mobile operating system
e the years the volume of malware targeting Android has conti

is is because it is easier and more profitable for malware auth
open source, more prevalent, and does not restrict the installa
art, numerous families of malware apps that are capable of inf
forming them into malicious bots have been discovered in th
acks such as Distributed Denial of Service (DDoS) attacks, ge

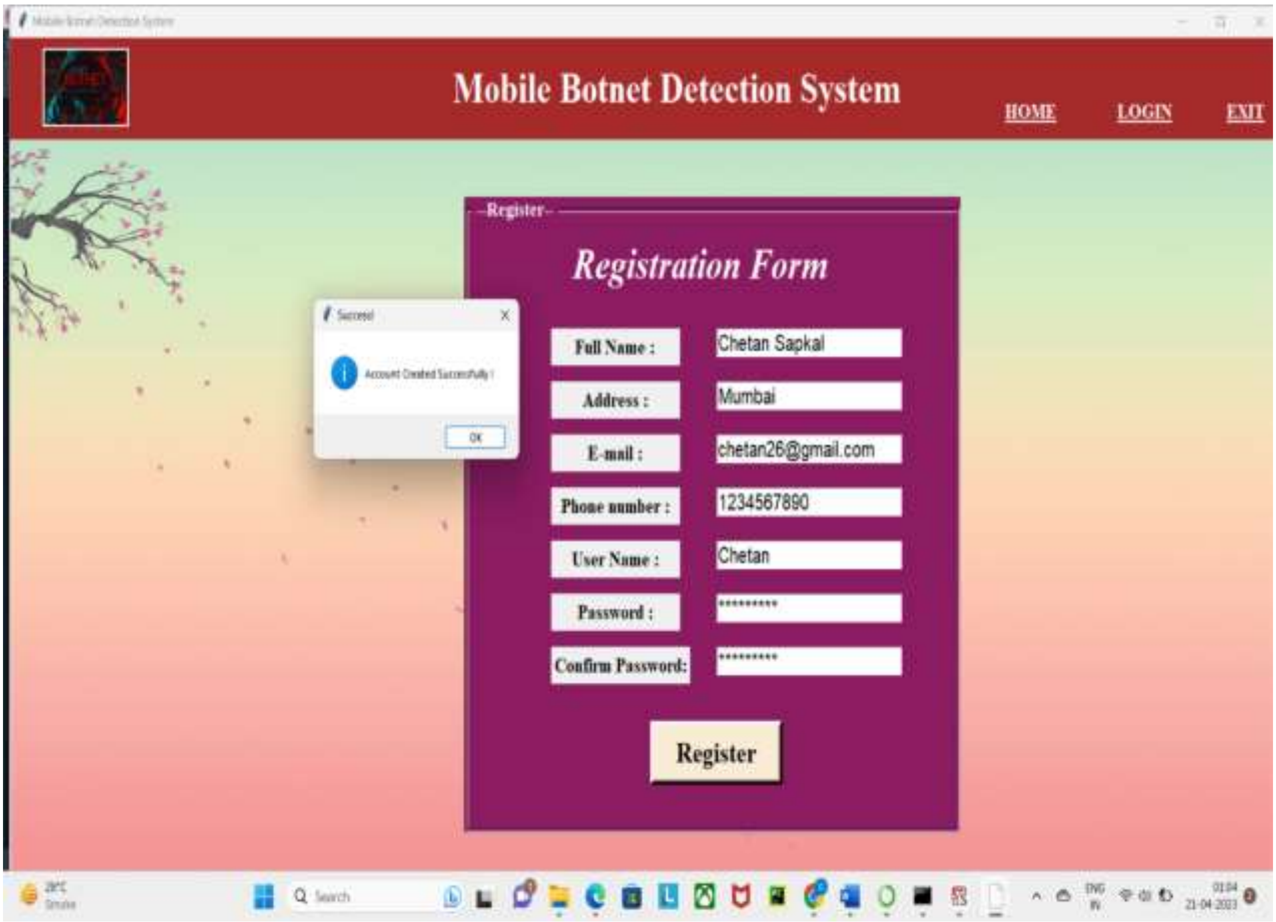
Figure 3.1: Front Page


Mobile Botnet Detection System
Mobile Botnet Detection System
HOME
REGISTER
EXIT
Login Here
Create Account
Login

Username: Chetan

Password: **********

Figure 3.2: Login Page



Registration Form

Full Name :	Chetan Sapkal
Address :	Mumbai
E-mail :	chetan26@gmail.com
Phone number :	1234567890
User Name :	Chetan
Password :	**********
Confirm Password:	**********

Account Created Successfully !

Register

Figure 3.3: Registration

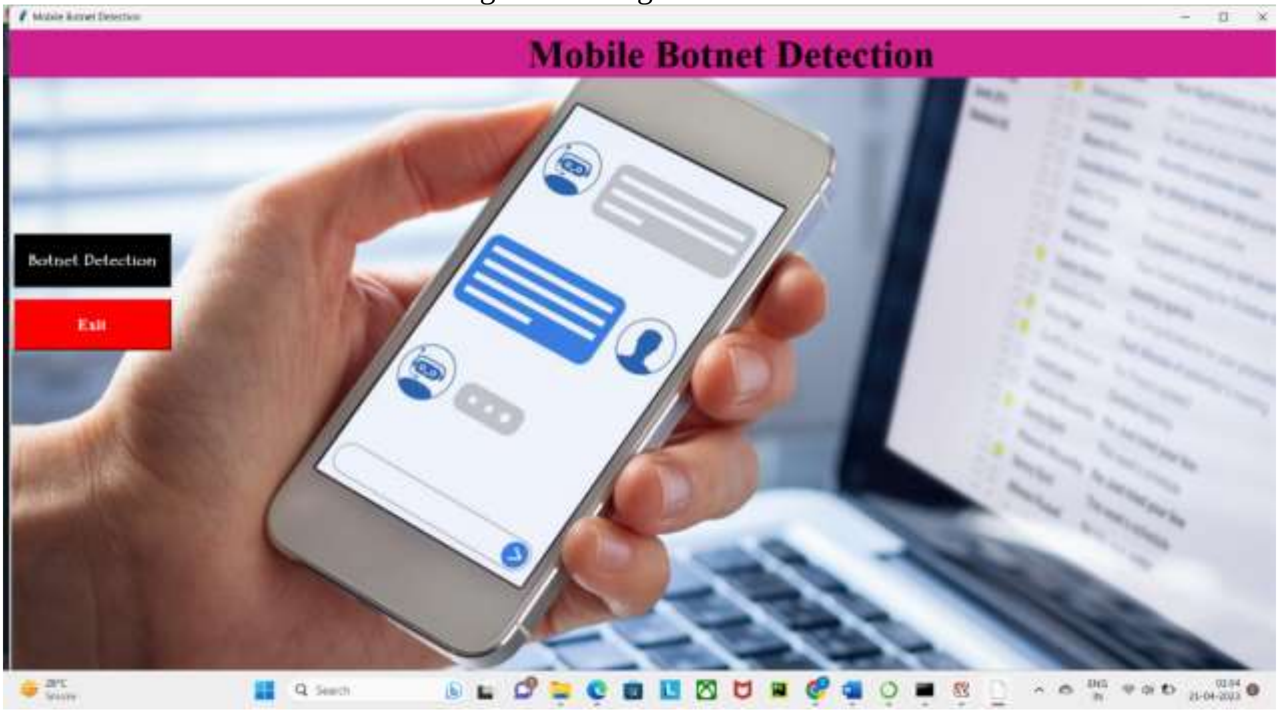
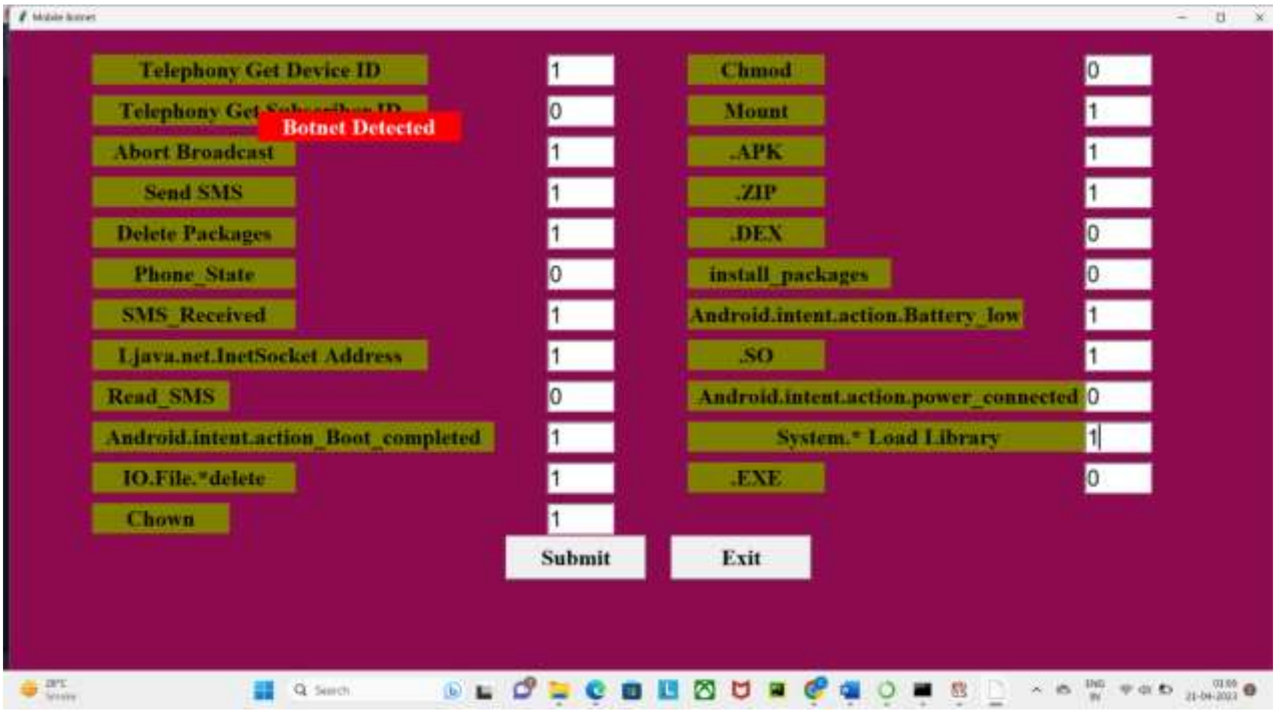


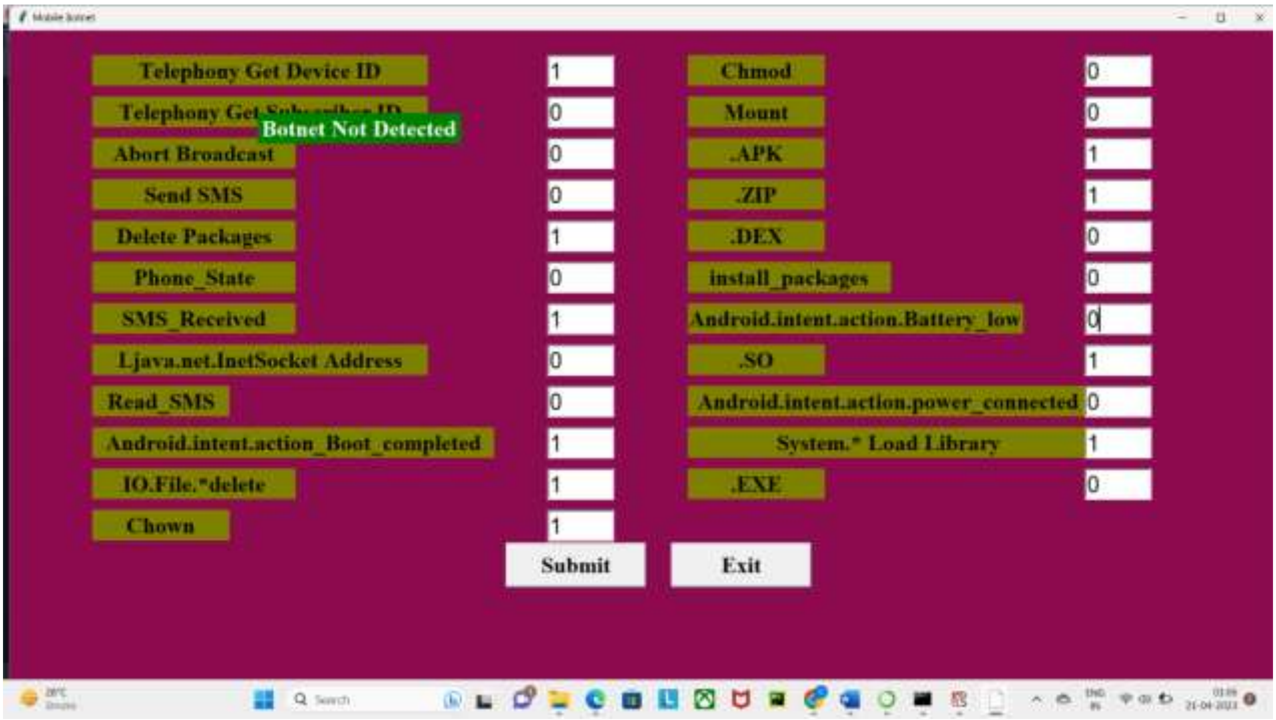
Figure 3.4: Main Page



Botnet Detected

Telephony Get Device ID	1	Chmod	0
Telephony Get Subscriber ID	0	Mount	1
Abort Broadcast	1	.APK	1
Send SMS	1	.ZIP	1
Delete Packages	1	.DEX	0
Phone_State	0	install_packages	0
SMS_Received	1	Android.intent.action.Battery_low	1
Ljava.net.InetSocket Address	1	.SO	1
Read_SMS	0	Android.intent.action.power_connected	0
Android.intent.action_Boot_completed	1	System.* Load Library	1
IO.File.*delete	1	.EXE	0
Chown	1		

Figure 3.5: Botnet Detected



Botnet Not Detected

Telephony Get Device ID	1	Chmod	0
Telephony Get Subscriber ID	0	Mount	0
Abort Broadcast	0	.APK	1
Send SMS	0	.ZIP	1
Delete Packages	1	.DEX	0
Phone_State	0	install_packages	0
SMS_Received	1	Android.intent.action.Battery_low	0
Ljava.net.InetSocket Address	0	.SO	1
Read_SMS	0	Android.intent.action.power_connected	0
Android.intent.action_Boot_completed	1	System.* Load Library	1
IO.File.*delete	1	.EXE	0
Chown	1		

Figure 3.6: Botnet Not Detected

3.5 Conclusion And Future work

Conclusion:

Botnets are a Dangerous evolution in the malware world. They are being used to damage systems, steal information and Comprise Systems. They are hard to detect and eliminate. So Our System Is Useful To detect Mobile Botnet.

Future work:

In this paper, we studied the classification and detection of botnet viruses. This malicious software is rapidly used by developers for application development, these led to an increase in the amount of malware in the system.Therefore, in future implementations, theproposed methodology will work for detecting the various types of botnet viruses. At the end of the studies, we will come to the conclusion that afeature selection-based system will build in the future.

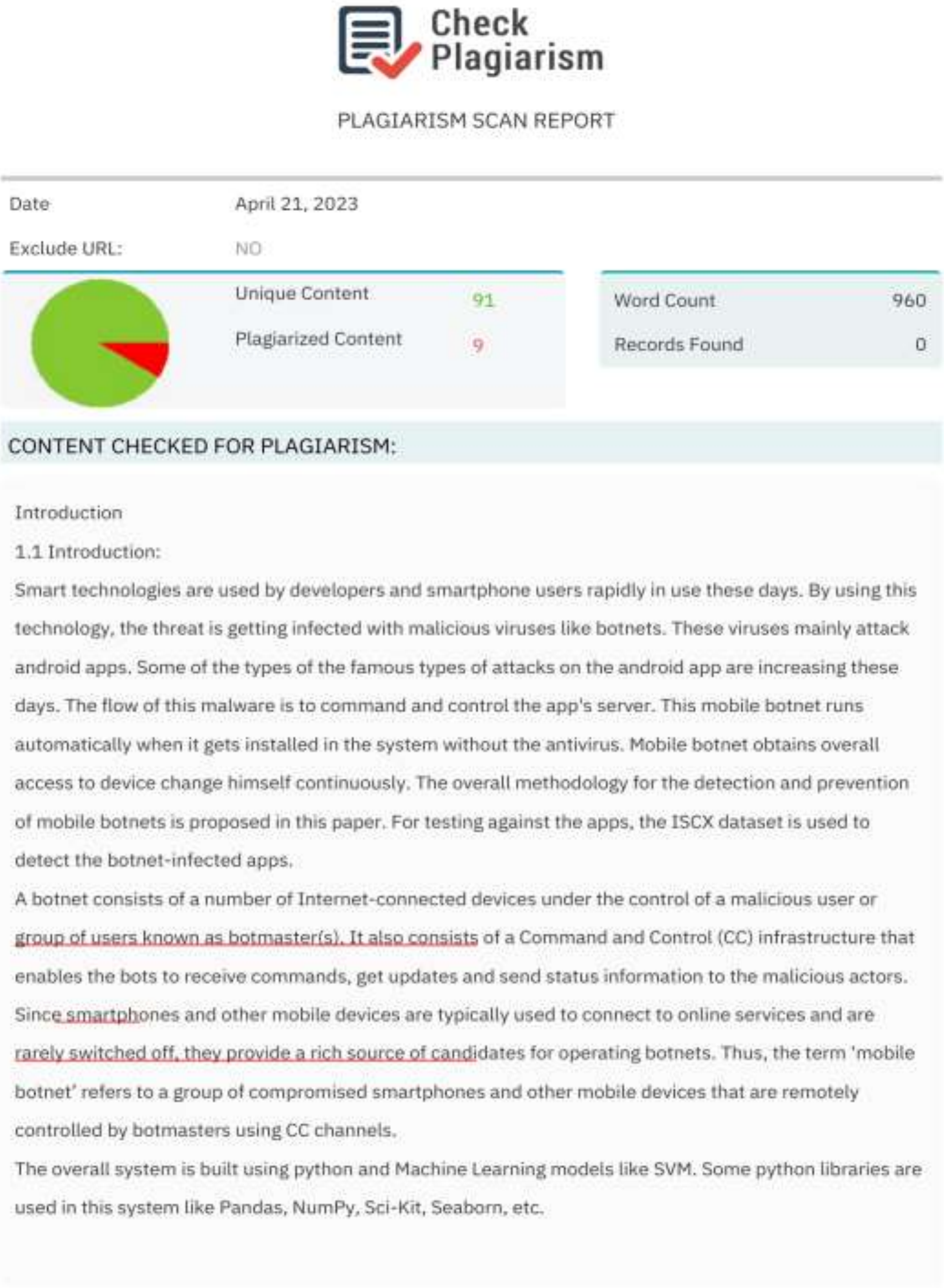
3.6 Conclusion & Future Enhancement

In conclusion, botnet detection is a critical component of cybersecurity, as botnets can be used to launch a wide range of malicious activities. Machine learning is a powerful tool for detecting botnet activity, as it can analyse large amounts of data and identify patterns and behaviour's that are indicative of botnet activity. However, there are several challenges involved in botnet detection, such as the ability of attackers to evade detection by using sophisticated techniques such as encryption and obfuscation.

To enhance botnet detection in the future, there are several areas that can be explored are: Integration with other security systems, Continuous monitoring, Improved feature extraction, Hybrid approaches and Collaboration.

In summary, the future of botnet detection will rely on ongoing research and development in the field of cybersecurity, as well as collaboration and cooperation between various stakeholders. By leveraging the power of machine learning and other advanced technologies, we can build more effective botnet detection systems to help protect against cyber threats.

3.7 Plagiarism Report



Check Plagiarism

PLAGIARISM SCAN REPORT

Date	April 21, 2023
Exclude URL:	NO

Unique Content	91
Plagiarized Content	9

Word Count	960
Records Found	0

CONTENT CHECKED FOR PLAGIARISM:

Introduction

1.1 Introduction:

Smart technologies are used by developers and smartphone users rapidly in use these days. By using this technology, the threat is getting infected with malicious viruses like botnets. These viruses mainly attack android apps. Some of the types of the famous types of attacks on the android app are increasing these days. The flow of this malware is to command and control the app's server. This mobile botnet runs automatically when it gets installed in the system without the antivirus. Mobile botnet obtains overall access to device change himself continuously. The overall methodology for the detection and prevention of mobile botnets is proposed in this paper. For testing against the apps, the ISCX dataset is used to detect the botnet-infected apps.

A botnet consists of a number of Internet-connected devices under the control of a malicious user or group of users known as botmaster(s). It also consists of a Command and Control (CC) infrastructure that enables the bots to receive commands, get updates and send status information to the malicious actors. Since smartphones and other mobile devices are typically used to connect to online services and are rarely switched off, they provide a rich source of candidates for operating botnets. Thus, the term 'mobile botnet' refers to a group of compromised smartphones and other mobile devices that are remotely controlled by botmasters using CC channels.

The overall system is built using python and Machine Learning models like SVM. Some python libraries are used in this system like Pandas, NumPy, Sci-Kit, Seaborn, etc.

3.8 Code

GUI_main.py

```
import tkinter as tk
#from tkinter import ttk, LEFT, END
from PIL import Image, ImageTk

root = tk.Tk()
root.configure(background="white")
# root.geometry("1300x700")

w, h = root.winfo_screenwidth(), root.winfo_screenheight()
root.geometry("%dx%d+0+0" % (w, h))
root.title("Mobile Botnet Detection System")



#For background Image
image2 = Image.open('slide.jpg')
image2 = image2.resize((w,h), Image.ANTIALIAS)

background_image = ImageTk.PhotoImage(image2)
background_label = tk.Label(root, image=background_image)
background_label.image = background_image
background_label.place(x=0, y=0)  # , relwidth=1, relheight=1)

label_l1 = tk.Label(root, text="Mobile Botnet Detection System",font=("Times New Roman", 30, 'bold'),
                 background="brown", fg="white", width=67, height=2)
label_l1.place(x=0, y=0)

img = Image.open('clogo.jpg')
img = img.resize((100,70), Image.ANTIALIAS)
logo_image = ImageTk.PhotoImage(img)
logo_label = tk.Label(root, image=logo_image)
logo_label.image = logo_image
logo_label.place(x=40, y=10)
frame_alpr = tk.LabelFrame(root, text=" --Details-- ", width=700, height=600, bd=5, font=('times', 14, ' bold '),bg="grey")
frame_alpr.grid(row=0, column=0, sticky='nw')
frame_alpr.place(x=800, y=150)
label_l2 = tk.Label(frame_alpr, text="Mobile Botnet Detection System \n \n \n Android is now the most widespread mobile operating system worldwide. \n Over the years the volume of malware targeting Android has continued to grow. \n \n This is because it is easier and more profitable for malware authors to target \n an operating system that is open-source, more
of fact, numerous families of malware apps that are  capable of infecting Android devices and
\n turning them into malicious bots have been discovered in the wild.\n These Android bots
may become part of a larger botnet that can be used to perform various types of attacks such as
Distributed Denial of Service (DDoS) attacks, generation and distribution of Spam, Phishing
attacks, click fraud, stealing login credentials or credit card details, etc.",font=("Times New
Roman",15, 'bold'),width=50,
            background="grey", fg="white")
label_l2.place(x=30, y=15)


img1 = Image.open('slide1.jpg')
img1 = img1.resize((750,600), Image.ANTIALIAS)
logo_image1 = ImageTk.PhotoImage(img1)

logo_label1 = tk.Label(root, image=logo_image1)
logo_label1.image = logo_image1
logo_label1.place(x=15, y=150)


def log():
    from subprocess import call
    call(["python","GUI_main.py"])
    root.destroy()

def window():
  root.destroy()

def login():
    from subprocess import call
    call(["python","login.py"])
    root.destroy()

def about():
    from subprocess import call
    call(["python","register.py"])
    root.destroy()
button1=tk.Button(label_l1,text="LOGIN", command=login, width=10, height=1,font=('times
15 bold underline'),bd=0, bg="brown", fg="white")
button1.place(x=750, y=70)

button2=tk.Button(label_l1,text="REGISTER",command=about,width=13,height=1,font=('ti
mes 15 bold underline'), bd=0,bg="brown", fg="white")
button2.place(x=850, y=70)

button4=tk.Button(label_l1,text="EXIT",command=window,width=10, height=1,font=('times
15 bold underline'),bd=0,bg="brown", fg="white")
button4.place(x=950, y=70)
```

```
label_l1 = tk.Label(root, text="** Mobile Botnet Detection System @2021 By ___
**",font=("Times New Roman", 10, 'bold'),
                  background="black", fg="white", width=250, height=2)
label_l1.place(x=0, y=800)

root.mainloop()
```

References

[1] S. Anwar, J. M. Zain, Z. Inayat, R. U. Haq, A. Karim, and A. N. Jabir, "A static approach towards mobile botnet detection," in 2016 3rd International Conference on Electronic Design (ICED), 2016: IEEE, pp. 563-567.

[2] Z. Abdullah, M. M. Saudi, and N. B. Anuar, ‘‘ABC: Android botnet classification using feature selection and classification algorithms,’’ Adv. Sci. Lett., vol. 23, no. 5, pp. 4717–4720, May 2017.

[3] S. Hojjatinia, S. Hamzenejadi, and H. Mohseni, ‘‘Android botnet detection using convolutional neural networks,’’ in Proc. 28th Iranian Conf. Electr. Eng. (ICEE), Aug. 2020, pp. 1–6.

[4] Kadir, A.F.A.; Stakhanova, N.; Ghorbani, A.A. Android botnets: What urls are telling us. In Proceedings of the International.

[5] Conference on Network and System Security, New York, NY, USA, 3–5 November 2015; Springer: New York, NY, USA, 2015; pp. 78–
91. ISCX Android Botnet Dataset. Available online: https://www.unb.ca/cic/dataset/android- botnet.html (accessed on 23 December 2020).

[6] N. Peiravian and X. Zhu, "Machine learning for android malware detection using permission and API calls," in Proc. of 25th International Conference Tools with Artificial Intelligence (ICTAI), IEEE pp. 300-305, 2013.

[7] S. V. Yerima, S. Sezer, G. McWilliams, and I. Muttik "A new android malware detection An approach using Bayesian classification, in Proc of 27th International Conference on Advanced Information Networking and Applications (AINA) IEEE pp. 121-128 2013.

[8] A. Karim, R. Salleh, M. K. Khan, A. Siddiqa, and K. K. R. Choo, "On the analysis and detection of mobile botnet applications Journal of Universal Computer Science, 22(4), 567-588 2016.

[9] Jadhav, S., Dutia, S., Calangutkar, K., Oh, T., Kim, Y.H., Kim, J.N., 2015. Cloud-based android botnet malware detection system, in: Advanced Communication Technology (ICACT), 2015 17th International Conference on, IEEE. pp. 347–352.

[10] Karim, Ahmad & Salleh, Rosli & Shah, Syed. (2015). DeDroid: A Mobile Botnet Detection Approach Based on Static Analysis. 10.1109/UIC-ATC ScalCom-CBDCom-IoP.2015.240.