IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 5, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105314 |

Mobile Botnet Detection System

Ashvini Ghotale, Gayatri Gavade, Vibhanshu Raj, Rahul Godage, Prof. B. B. Gite

Dept. of Computer Engineering, ISBM College of Engineering, Pune, India

Dept. of Computer Engineering, ISBM College of Engineering, Pune, India

Dept. of Computer Engineering, ISBM College of Engineering, Pune, India

Dept. of Computer Engineering, ISBM College of Engineering, Pune, India

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 plat- form. 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.

KEYWORD: Botnet detection, Android Botnets, Deep learning, Convolutional, Neural Networks, Machine learning.

I. INTRODUCTION

1.1 OVERVIEW

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.

1.2 Motivation

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

1.3 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.

1.4 PROBLEM STATEMENT

In This project we Detect Botnet App. Botnet App Means Some malwares are in- stalled 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.

II.RELATED WORK

First we take some project Topic with its reference paper then we finalize one of the easy and useful project which is mobile malware detection. Because now day security is very important in all areas. Then we take some research paper for knowing some more information about the mobile malware detection system .then we will start the coding of our project .till now we will make registration page and login page for our project security. We will use tk inter library for making login page and registration page. this project will make in machine learning but there is more error so in this project we solve it we use python for this project.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105314 |

III.PROPOSED METHODOLOGY

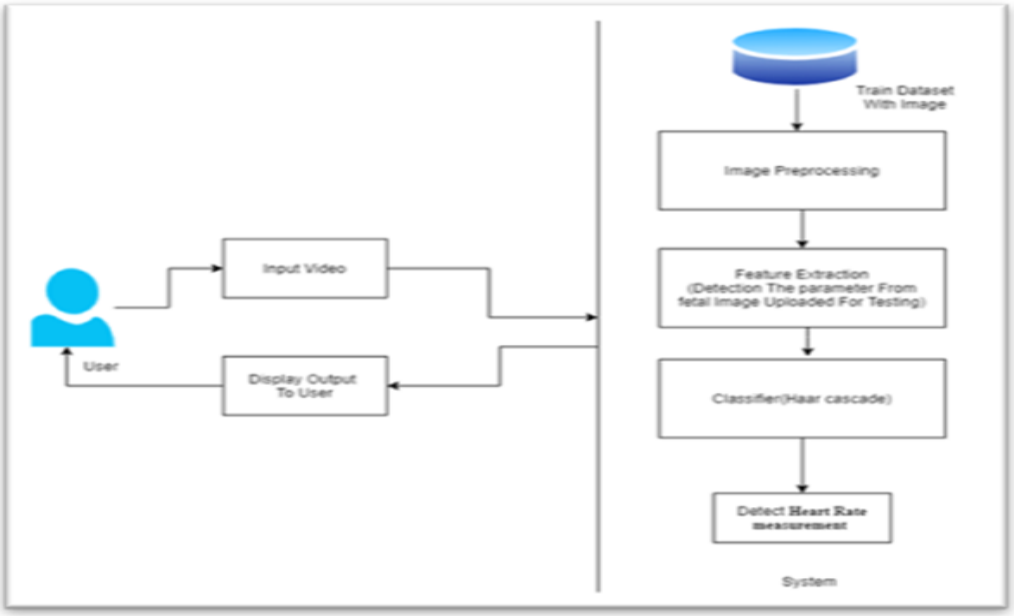
1) **A.Block Diagram Description**

A. • Admin

In this module, the Admin has to log in by using valid user name and password.

After login successful he can do some operations such as View All Users and Authorize, View All E-Commerce Website and Authorize, View All Products and Reviews, View All Products Early Reviews, View All Keyword Search Details, View All Products Search Ratio, View All Keyword Search Results, View All Product Review Rank Results. •View and Authorize Users.

B. System architecture Diagram



| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105314 |

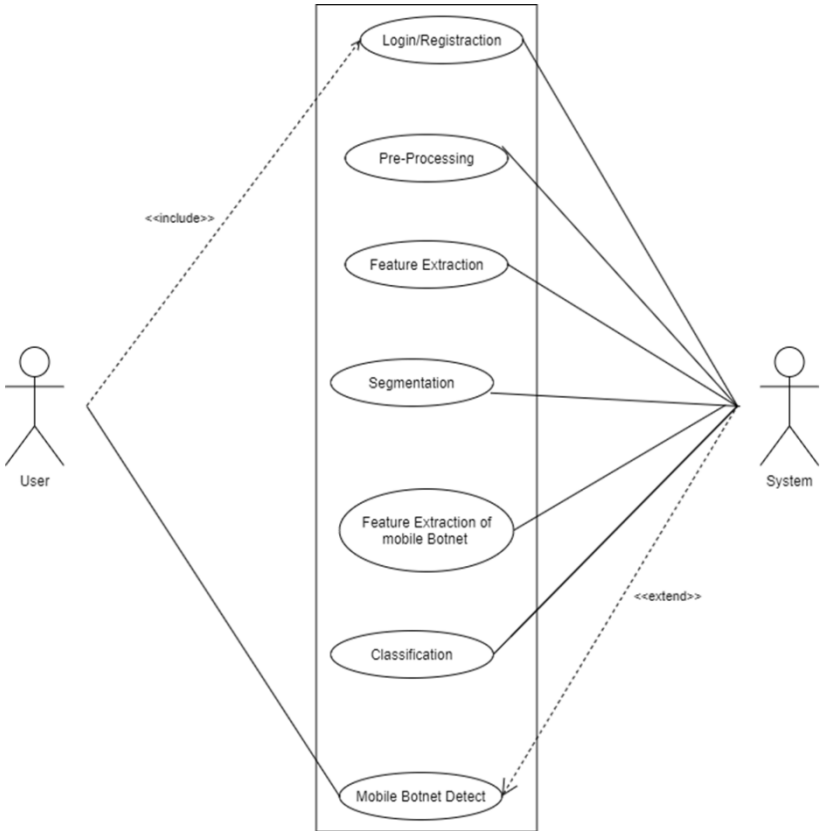
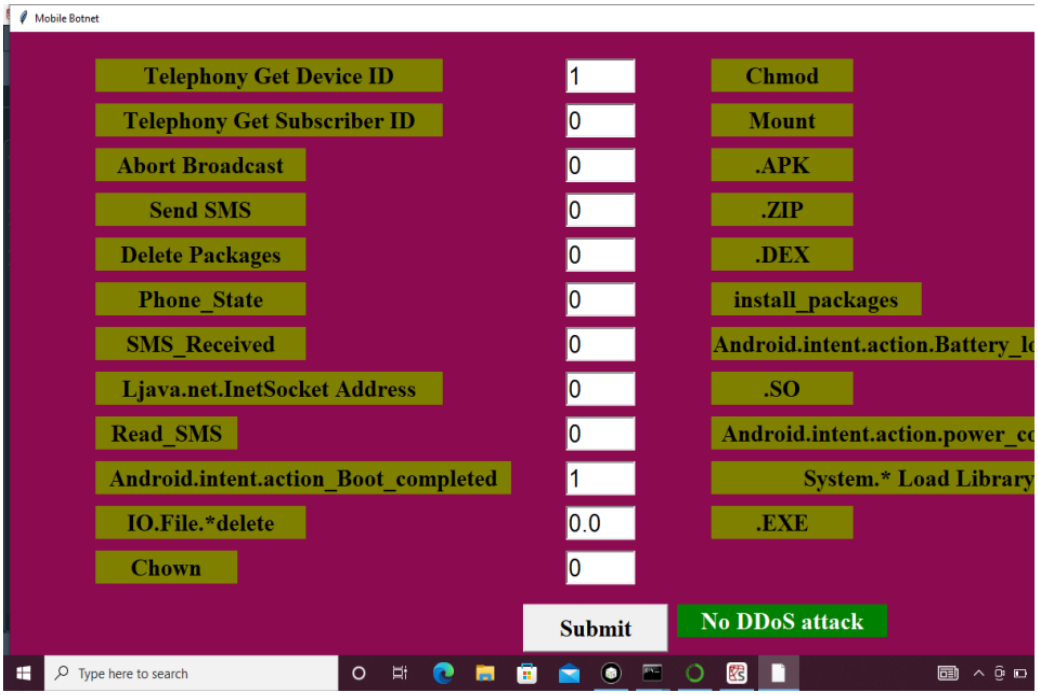


Fig. 5. Power Supply

IV. RESULT



| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105314 |

V.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. As smartphones become more popular, they become victims of potential attacks. With the openness of the Android OS design and its growing popularity, the growth of unprofessional Android software can be expected. In this paper specific trends and features of Android botnets have been identified. These can assist in the identification of current Android botnet and prevent the proliferation of new Android botnets. Future research includes an early study of the internal functionality of the current Android botnet and a malware program. The purpose of this study is to examine the development and basic structure of Android botnets to assist in the process of acquiring such botnet. A future focus will be on identifying Android botnet using a signature and / or behavioural-based acquisition model.

REFERENCES

[1]. 1 S. Y. Yerima and S. Khan "Longitudinal Performance Analysis of Machine Learning based Android Malware Detectors" 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), IEEE
[2]. H. Pieterse and M. S. Olivier,"Android botnets on the rise: Trends and characteristics," 2012 Information Security for South Africa, Johannesburg, Gauteng, 2012, pp. 1-5.
[3]. Letteri, I., Del Rosso, M., Caianiello, P., Cassioli, D., 2018. Performance of botnet detection by neural networks in software-dened networks, in: CEUR WORKSHOP PROCEEDINGS, CEUR-WS.
[4]. Kadir, A.F.A., Stakhanova, N., Ghorbani, A.A., 2015. Android botnets: Whaturls are telling us, in: International Conference on Network and System Security, Springer. pp. 78–91.
[5]. ISCX Android botnet dataset. Available from https://www.unb.ca/cic/datasets/androidbotnet.html. [Accessed 03/03/2020]
[6]. M. Eslahi, M. V. Naseri, H. Hashim, N. M. Tahir, and E. H. M. Saad, "BYOD: Current State and Security Challenges," presented at the IEEE Symposium on Computer Applications Industrial Electronics, Peneng, Malaysia, 2014
[7]. S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, "Botnets: A survey," Computer Networks, vol. 57, pp. 378-403, 2013
[8]. A. J. Alzahrani and A. A. Ghorbani, "SMS mobile botnet detection using a multi-agent system: research in progress," presented at the Proceedings of the 1st International Workshop on Agents and Cybersecurity, Paris, France, 2014
[9]. G. Gu, J. Zhang, and W. Lee, "BotSniffer: Detecting botnet command and control channels in network traffic," in Proceedings of the 15th Annual Net- work and Distributed System Security Symposium (NDSS'08), 2008
[10]. C. Byungha, C. Sung-Kyo, and C. Kyungsan, "Detection of Mobile Botnet Using VPN," in Proceedings of the Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013, pp. 142-148

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details