Mobile Botnet Detection Using ConvolutionalNeural Networks

1st Prof. Dr. Sachin Sukhadeo Bere | sachinbere@gmail.com 2nd Prof. Swati Mahadev Atole | smatole.foe@dattakala.edu.in 3rd Vaishnavi Haribhau Awari | awarivaishnavi6@gmail.com 4th Pradnya Baban Kalange | pradnyakalange1212@gmail.com5th Sanjivani Shivaji Munde | mundesanjivani09@gmail.com 6th Supriya Hirachand Phalle | supriyaphalle222@gmail.com

Department Of Computer Engineering
Dattakala Group of Institutions Faculty of Engineering
Pune-Solapur Highway, Swami-Chincholi (Bhigwan), Tal-Daund, Dist-Pune-413130Email ID-dkcom.edu@rediffmail.com

Abstract:
Botnets have been a serious threat to the Internet security. With their constant sophistication and the resilience of them, a new trend has emerged, shifting botnets from the traditional desktop to the mobile environment. As in the desktop domain, detecting mobile botnets is essential to minimize the threat that they impose. Along the diverse set of strategies applied to detect these botnets, the ones that show the best and most generalized results involved is- covering patterns in their anomalous behavior. In the mobile botnet field, one way to detect these patterns is by analyzing the operation parameters of this kind of application. In this paper, we present an anomaly-based and host-based approach to detect mobile botnets. The proposed approach uses machine learning algorithms to identify anomalous behaviors in statistical features extracted from system calls. We were able to test the performance of our approach in a close-to reality scenario. The proposed approach achieved great results, including low false positive rates and high true detection rates. Index Terms—Machine learning, Deep learning, Convolutional Neural Networks (CNN), Botnet Detection, etc.

1. Introduction

Due to the increase of mobile phone users and the increasing number of Android market share nowadays, we noticed that the number of Android malware is also apparently increasing. we extract important features from the Android APK files that can be used to identify a botnet andits family. we find an appropriate machine learning algorithm to classify the Android botnet family with a high recall, and lastly. we developed a system called ABIS (Android Botnet Identification frustum) that includes the identification engine, a web application, and an Android applicationfor the users to check any application before installing it. The rest of this paper is organized as follows.

2. LITERATURE SURVEY

A research paper is a document of a scientific article that contains relevant expertise, including substantive observations, and also references to a specific subject of philosophy and technique.

1) ABIS: A Prototype of Android Botnet Identification System:- According to the advanced wire-less technology in nowadays, most people mainly use their mobile phones as an essential tool. At the same time, threats to mobile phones such as viruses, botnets, and other malwareare also increasing . However, most users have limited knowledge about mobile threats. Therefore, we would like to reduce the

number of botnet-infected mobile phones before the users install an application on their phones. We developed a system called ABIS (Android

Botnet Identification System) to check Android applications and whether they are possibly malware or not. To identify the Android botnets, our system learns the characteristics of each Android botnet family from the dataset provided by the University of New Brunswick . We analyze the Android APK files, extract important features, and find an appropriate machine- learning technique. As a result, we found that our system can classify the Android botnets with about 96.9 of recall.

2) ABC: Android Botnet Classification Using Feature Selection and Classification Algorithms:- Smartphones have become an important part of human lives, and this led to an increase number of smartphone users. However, this also attracts hackers to develop malicious ap- plications especially Android botnets to steal private information and cause financial losses.Due to the fast modifications in the technologies used by malicious application (app) devel- opers, there is an urgent need for more advanced techniques for Android botnet detection. In this paper, a new approach for Android botnet classification based on features selection and classification algorithms is proposed. The proposed approach uses the permissions requested in the Android app as features, to differentiate between the Android botnet apps and benign apps. The Information Gain algorithm is used to select the most significant permissions, and then the classification algorithms Na¨ıve Bayes, Random Forest, and J48 used to classify Android apps as botnet or benign apps. The experimental results showthat the Random Forest Algorithm achieved the highest detection accuracy of 94.6 with the lowest false positive rate of 0.099.
3) Toward a Detection Framework for Android Botnet:- 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 a 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 on a new setof discriminating features extracted from the analysis of Android permissions (i.e. Protectionlevels 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 Na¨ıve Bayes)for our experiments and we found that the new set of features have a tiny improvement in the performance in the case of decision trees and Random forest classifiers
4) Mobile Botnet Detection: A Deep Learning Approach Using Convolutions Neural Networks:-Android, being the most widespread mobile operating system 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 com-pared 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) Detection of Mobile Botnets using Neural Networks:- 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 behavior because they are not managed by predictable algorithms but they are controlled by humans via command and control servers (CC servers) or via peer-topper networks. However, they have certain common features which have been revealed by analysis of contemporary mobile botnets.

These features have been used for the 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

3. PROPOSED SYSTEM

3.1. *System Architecture*

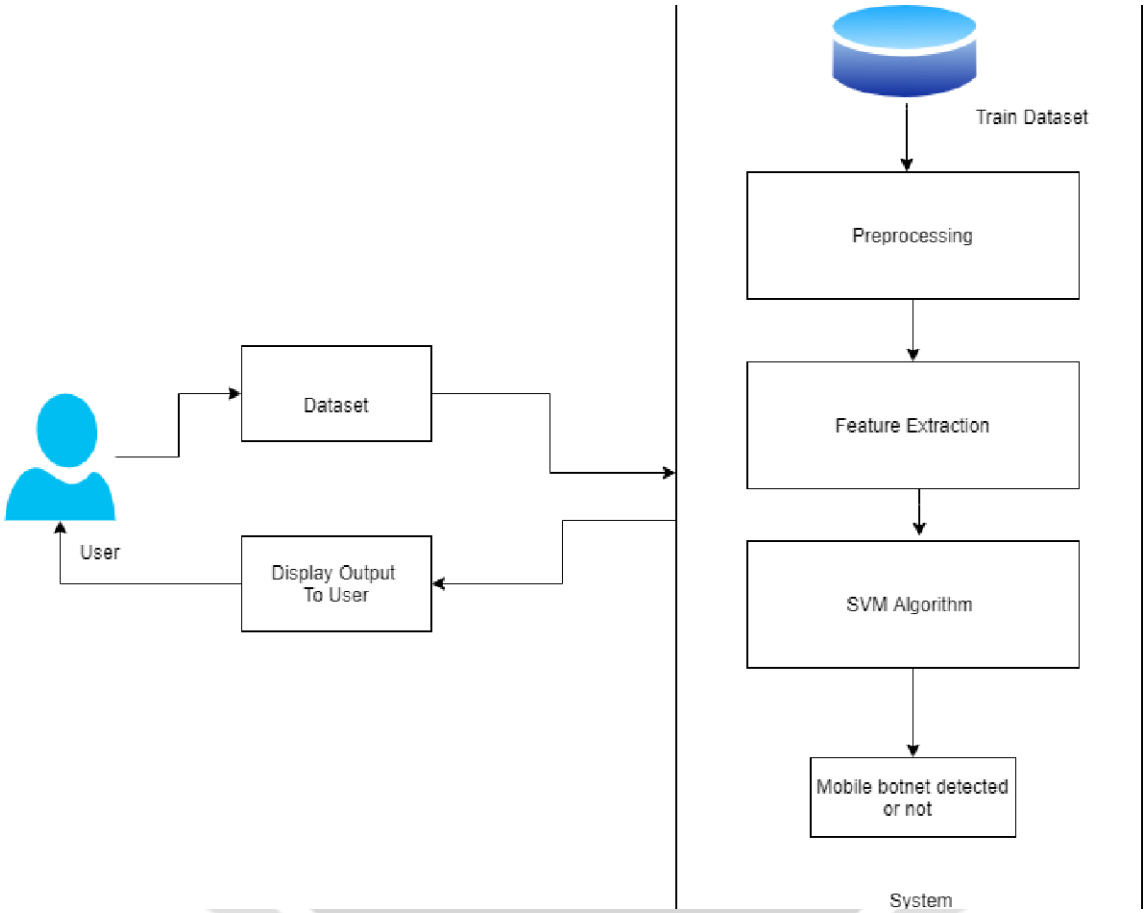

Fig. 1. System Architecture of Mobile Botnet Detection

3.2. *data flow diagram*

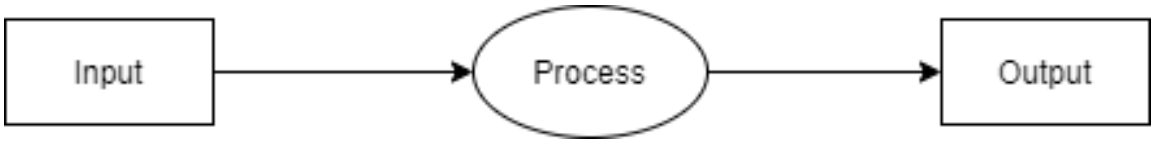

Fig. 2. Data flow diagram 0

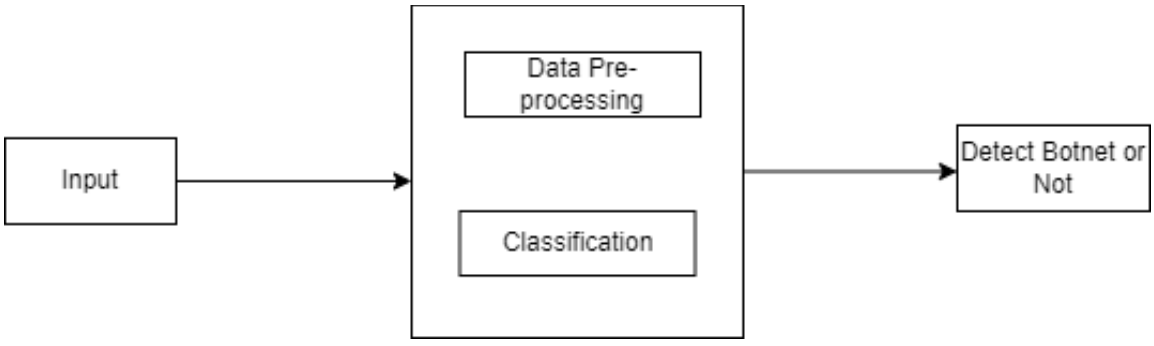

Fig. 3. Data flow diagram 1

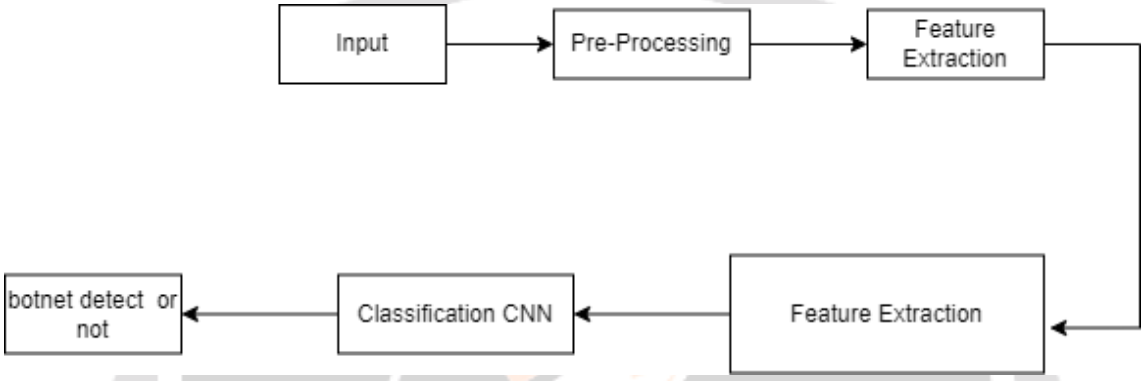

Fig. 4. Data flow diagram 2

3.3 class diagram

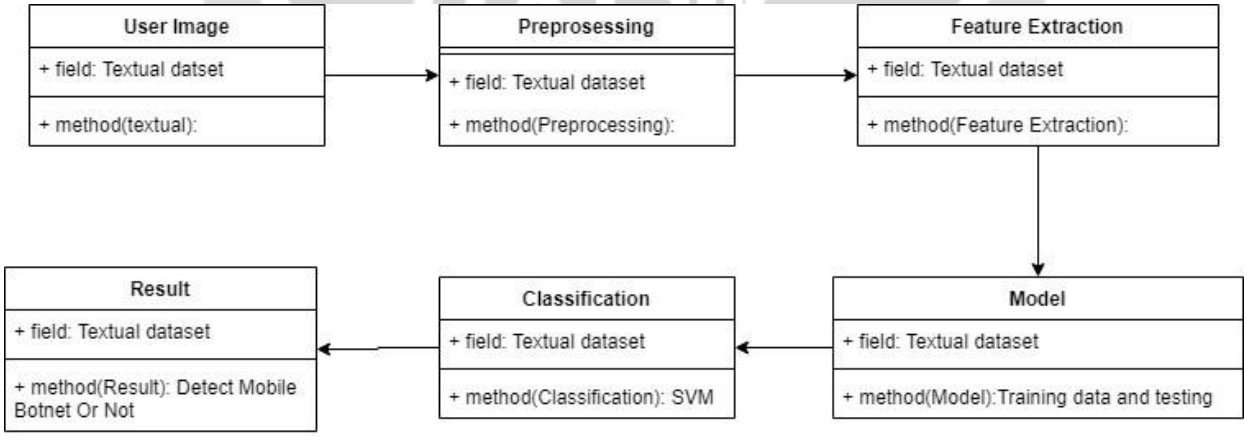

Fig.5. Class diagram

3.4 *Use case diagram*

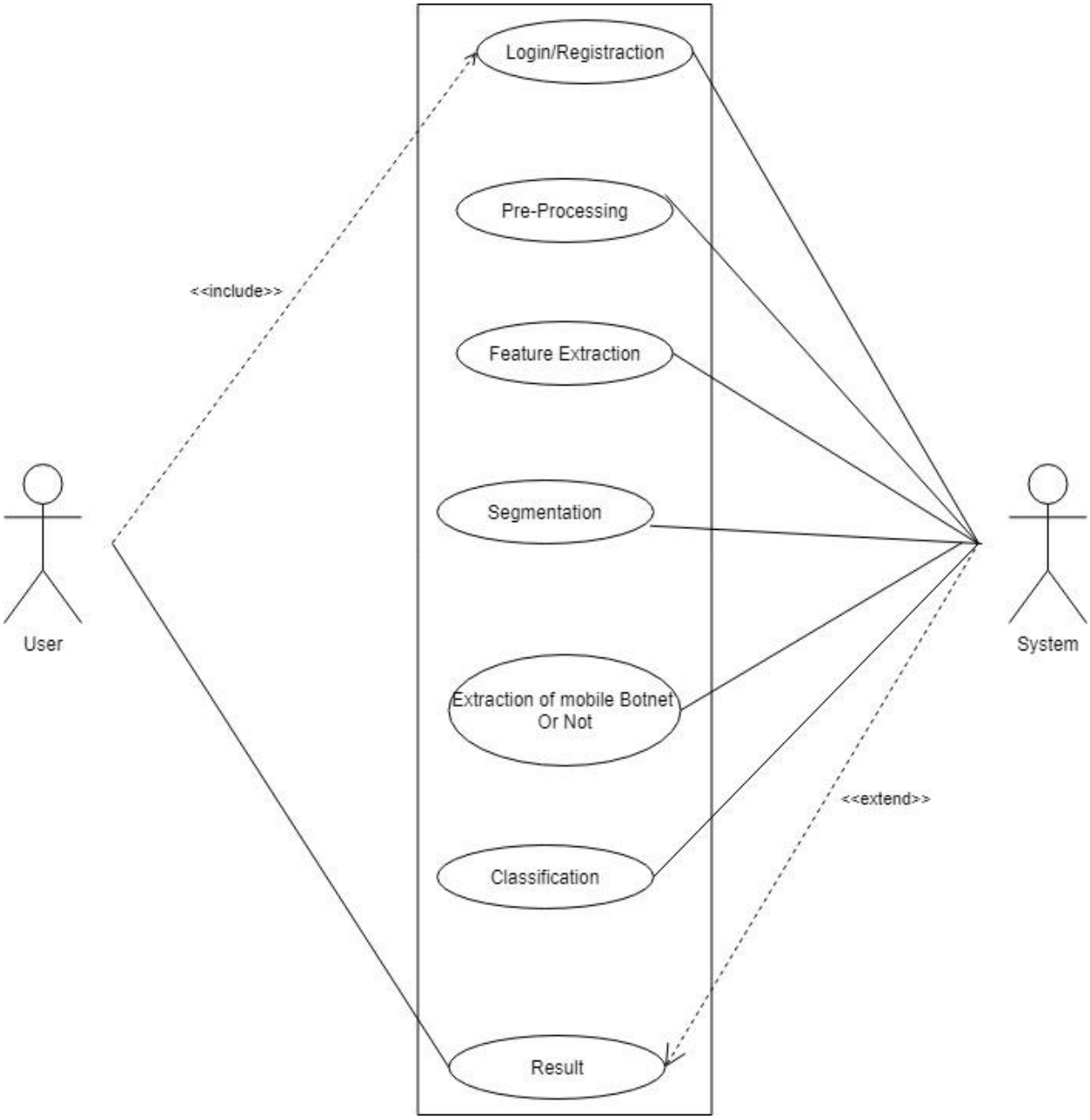

Fig.6. Use case diagram

4. RESULT

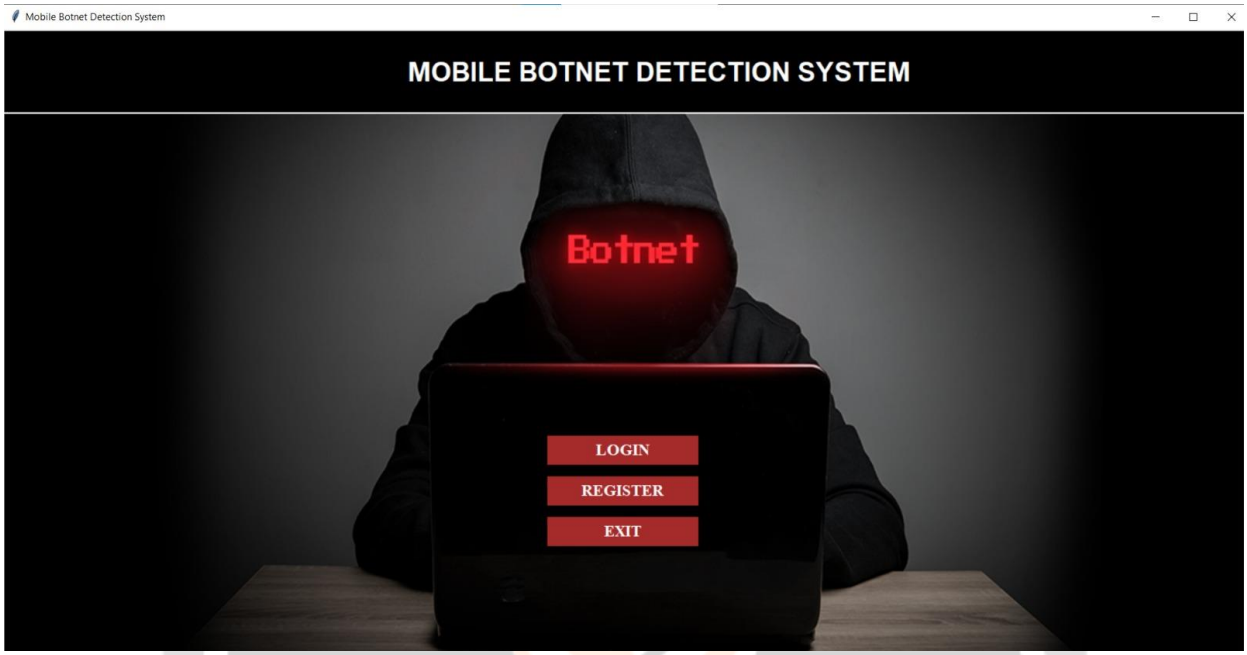

Fig.1. Home Page

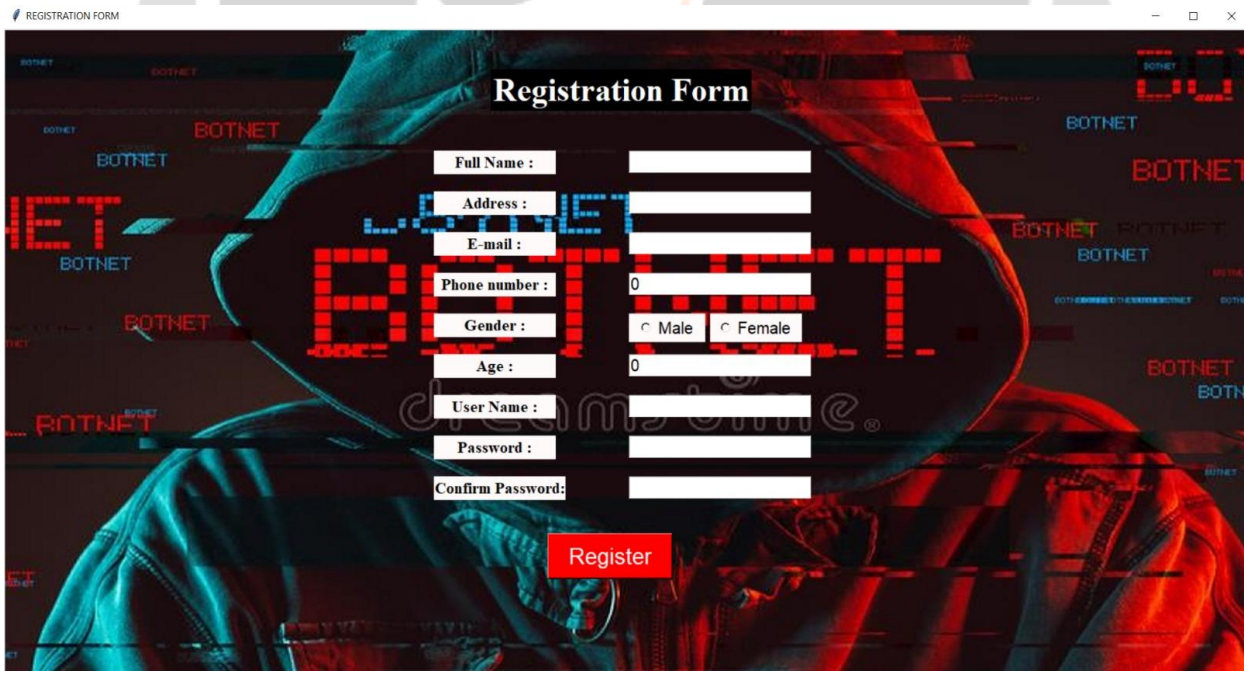

Fig.2. Registration page

Fig.3 Login Page

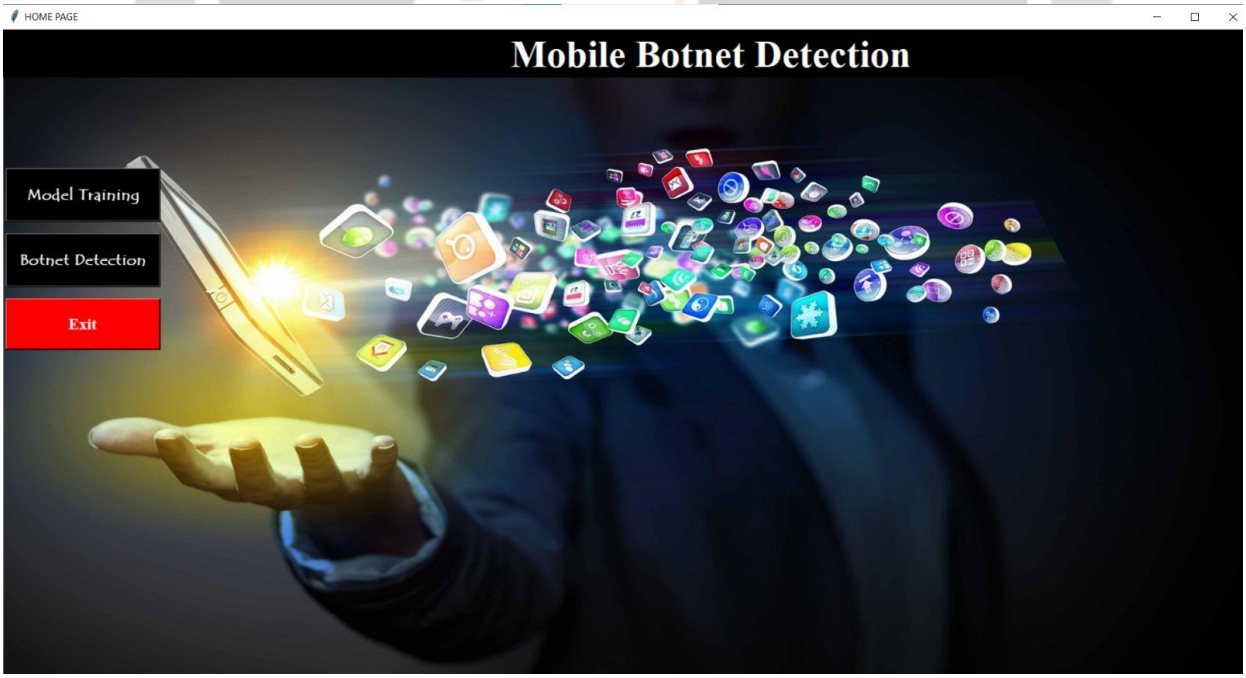

Fig.4. Botnet detection home page

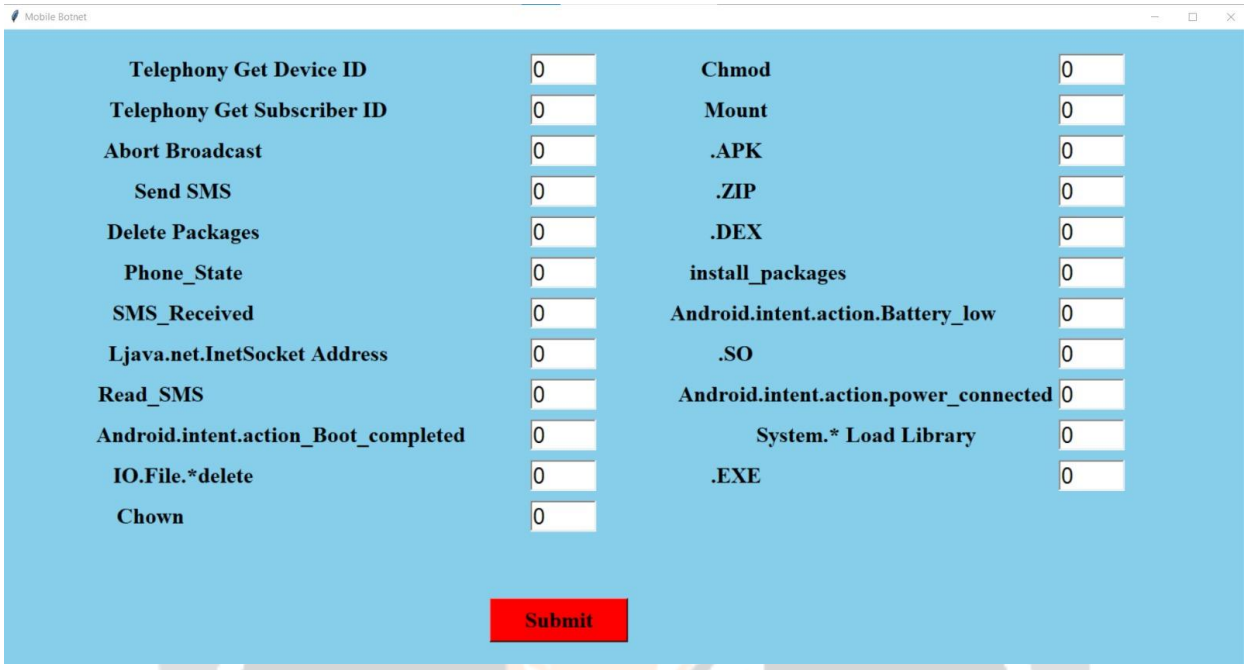

Fig.5. Botnet detection page

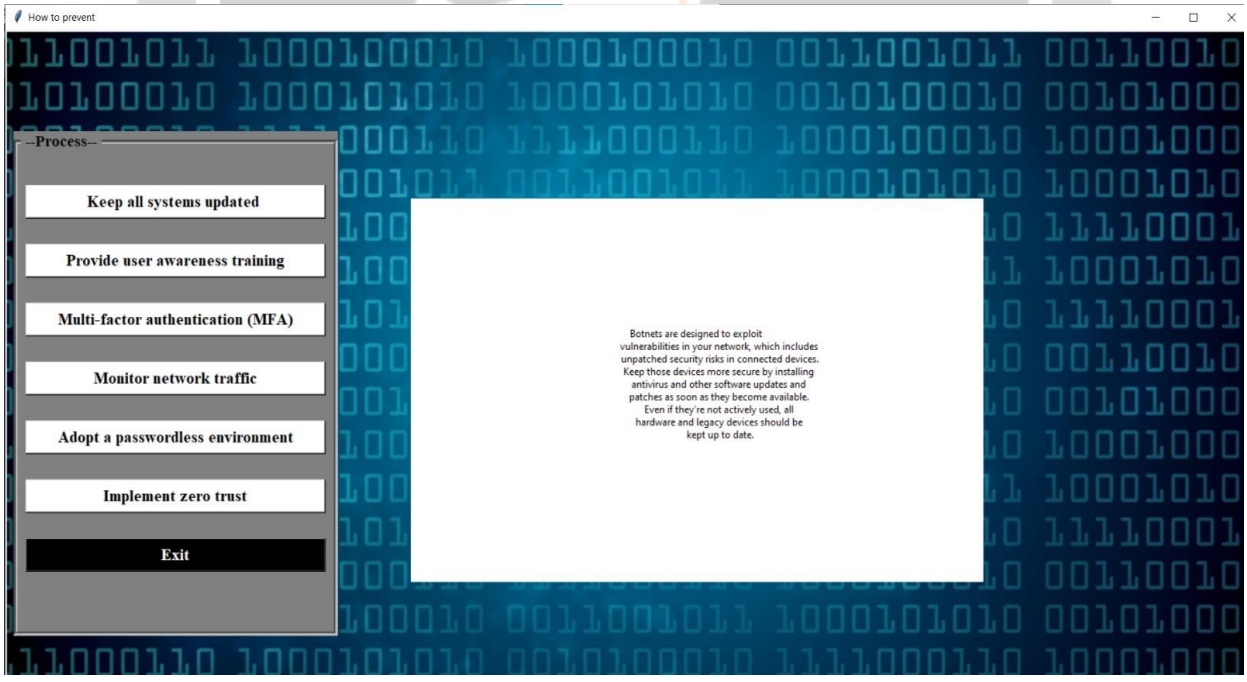

Fig.6. Botnet prevention page

5. ADVANTAGES

- Mobile botnets take advantage of unpatched exploits to provide hackers with root permissionsover the compromised mobile device, enabling hackers to send email or text messages, makephone calls, access contacts and photos, and more
- Provide more security
- Easy to handle

6. USE OF APPLICATION

- Company
- In Office
- In Banking
- All User

7. 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

8 . FUTURE WORK

With just one neural network, it is feasible to recognize features from both sets. To estimate the natural ratio of these sets, a static analysis of both sets with a significant number of samples is required (such that the central limit theorem is valid). The training set will be constructed in such a way that vectors with this ratio are included.

9. REFERENCES

3.1. 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.

3.2. Kadir, A.F.A., Stakhanova, N., Ghorbani, A.A., 2015. Android botnets: What URLs are tellingus, in: International Conference on Network and System Security, Springer. pp. 78–91

3.3. 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

3.4. J. f. Alqatawna and H. Faris, ”Toward a Detection Framework for Android Botnet,” in 2017 International Conference on New Trends in Computing Sciences (ICTCS), 2017: IEEE, pp. 197- 202

3.5. Letteri, I., Del Rosso, M., Caianiello, P., Cassioli, D., 2018. Performance of botnet detection by neural networks in software-dened networ

3.6. S.Y. Yerima and S. Khan “Longitudinal Performance Analysis of Machine Learn-based An- droid Malware Detectors” 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), IEEE

3.7. ISCX Android botnet dataset. Available from https://www.unb.ca/cic/datasets/androidbotnet.html. [Accessed 03/03/2020]

3.8. S Hojjatinia, S Hamzenejadi, H Mohseni, “Android Botnet Detection using Convolutional Neural Networks” 28th Iranian Conferenc on Electircal Engineering (ICEE2020)