International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Android Botnet Detection Using Machine Learning

[1]Prof. Suhas Chavan, [2]Mayur Jagadale, [3]Arjun Shinde, [4]Swati Hande, [5]Ramakant Dhumal

[1,2,3,4,5] Department of Computer Engineering, STE'S SKN Sinhgad Institute of Technology and Science

ABSTRACT

A botnet is a widely spreading malware among mobile applications which is dangerous to mobile apps. Nowadays developers are widely using malicious software for fast development and good results, this leads to the spreading of botnet malware. A botnet mainly aims to hack the entire system and abduct the details of the user. By applying the proposed methodology and algorithms for the detection of botnets. By applying the Machine learning algorithm to the predefined datasets and got the conclusion of successfully testing against the dataset, and detecting some botnet-infected apps.

Keywords: Machine Learning, Botnet Detection, Android Botnet, Smart Framework, Algorithm.

I. 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.

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. the Structure is distributed in the following manner, in the section, I containing the introduction related to the paper. Section II is related to the actual implementation of the project. The methodology and the flow of the project are contained in section III. Section, IV contained the literature survey related to our proposed system. the V section contains the future scope of our project. The conclusion is written in section VI. In the end, the last section VII contains references related to our project.

II. Related Work

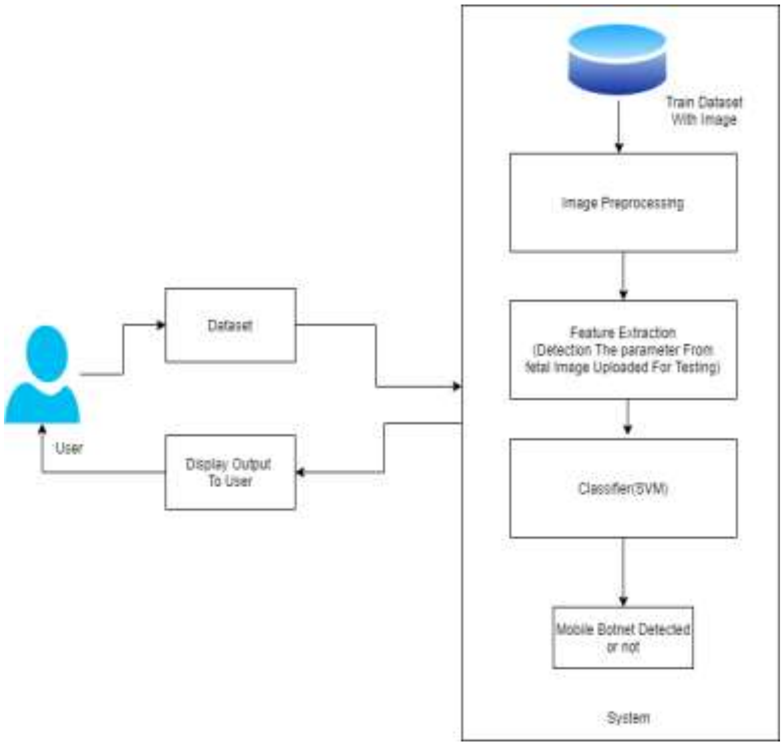
A botnet is a network of computers that are affected by botnet malware and remotely controlled by the hacker. The nature of a botnet is to change continuously when moving from one system to another. India is the largest country which are using various applications for growing in the IT industries.

According to the base paper [10], the work-related to the mobile botnet detection approach. The approach which was built in this paper DeDriod. DeDriod is for investigating the properties of mobile botnets for classification and detection.

Paper [11] used a machine-learning approach for the detection of an android botnet. The approach and the proposed work were done in this paper with some permission level which was some 147 permissions. There is a series of Machine Learning algorithms: Random Forest, NLP, Decision Tree & Naive Bayes. Using these algorithms increases the accuracy of the detection of botnet apps.

In another paper [6] Yerima proposed a model for android application to extract most important feature of the android application or the android operating system. Android malware detection using permission and api calls methodology was proposed in paper [7] by Peiravian and Zhu for the Permission and the feature combination in android. The Study which was done in this paper is related to the malware application and malicious software's.

III. Methodology



In Fig.1 Shows that there is a user who is affected by the botnet malware. it consists of train datasets, and with the help of that, we perform the detection of the infected apps. In this paper, the feature extraction methodology is used with the Support Vector Machine to detect botnet-infected apps. for our model, the ISCX dataset is used to test the botnet applications this dataset contains botnet-infected apps and our proposed methodology is used to detect it. this proposed methodology is built by using python and its frameworks. some python libraries are used in this model like pandas, NumPy, seaborn, SNS, etc. This model is built for windows based operating systems with a ram of 8 GB. The SVM classifier model is used to detect the real-time botnet apps with the train dataset using train dataset. the overall performance of the software will enable to the work anciently. This is the overall implementation of the proposed methodology.

IV. Literature Survey

in paper [1] we studied that the botnet detection in this paper is based on the feature extraction of android devices. The framework which is used in this paper has five layers of mobile security that can detect applications which are containing mobile botnets. these five layers are decompiler, extractor, smart learner, feature refine, and machine learning module.

Paper [2] it is demonstrated the study of botnet detection on Android based on the proposed system of Bot-Image framework, which is enabled by automated reverse engineering of android applications, image generation, and subsequent extraction of image-based and manifest features. The presence of a feature is denoted by 255 while a 0 is recorded if the feature is absent and these are stored in an array of manifest features.

The paper [3] says that the study is done using a learning-based Android detection system designed for the difference between clean apps and botnet apps. The various accuracy metrics used in this experiment presented the reuse obtained from the CNN-GRU model where the configuration of both the CNN layers and GRU layers were varied. The classification system is implemented by extracting steps features from thousands of applications consisting of both botnet and clean apps.

V. Future Scope

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, the proposed methodology will work for detecting the various types of botnet viruses. At the end of the studies, we will come to the conclusion that a feature selection-based system will build in the future.

VI. 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 Botnets.

VII. 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.

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

12] M. K. Alzaylaee, S. Y. Yerima, Sakir Sezer “DL-Droid: Deep learning based android malware detection using real devices” Computers & Security, Volume 89, 2020, 101663, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2019.101663.