Volume 9, Issue 05, May 2024 ISSN (online): 2456-0006

International Journal of Science Technology Management and Research

Available online at: www.ijstmr.com

A Study on Mobile Botnet Detection System

Yashashri H. Anare
MSC (Computer Science)
Indira College, Malegaon

Prof. Tushar. P. Sharma
MSC (Computer Science)
Indira College, Malegaon

Abstract-: We inhabit an era dominated by digital advancements, where an overwhelming flood of data and information is generated and processed daily. This vast reservoir of data serves myriad purposes, including scientific and medical research, news dissemination, blogging, and the compilation of constantly evolving statistical data. Consequently, comprehending and categorizing this multitude of data becomes progressively arduous, particularly given the propensity for errors and oversights when tackled manually. Such manual processes not only consume significant time but also lead to the proliferation of extraneous information at the expense of essential insights. Indeed, manually sifting through voluminous documents to extract meaningful summaries presents a formidable challenge for humans. Consequently, there arises a pressing need to devise a solution that swiftly and efficiently sifts and organizes pertinent information. To address these challenges, we propose the implementation of a text summarization model integrating TFIDF, Textrank algorithms, and various natural language processing techniques. This approach promises more precise outcomes compared to previous models, thereby facilitating streamlined access to relevant and actionable information across all domains. Furthermore, this solution holds the potential to expedite the identification of nefarious botnets that pose threats to data security and system integrity. Importantly, the time and effort saved by our solution not only enhances operational efficiency but also translates into substantial cost savings.

Keywords-: Machine Learning, Support Vector Machine (SVM), Botnet Detection, Deep Learning.

I. INTRODUCTION

The effective organization of information is pivotal in decision-making, problem-solving, and trend forecasting based on statistical data. This precision in data processing not only saves companies money and enhances decision-making but also underpins everyday choices for students, businesses, and educators alike. Mishandling raw data can lead to misleading outcomes and negative impacts on decisions. Consequently, there's a pressing need to delve deep into the issue and devise innovative, sustainable solutions. With the surge in mobile device usage, particularly Android smartphones, the risk of malware is widespread. Our system aims to extract crucial features from Android APK files to identify botnets accurately, including their class and family. By employing a suitable machine learning algorithm, we aim to segregate Android botnet families with high recall rates. The culmination of this effort is ABIS (Android Botnet Identification System), comprising an identification engine, web application, and Android app. ABIS empowers users to swiftly inspect and scan applications before installation, addressing both data refinement needs and security concerns. The escalating threat of malicious botnet applications demands more effective detection methods. Therefore, we propose a deep learning approach utilizing Convolutional Neural Networks (CNN) for Android botnet detection. Leveraging 342 static characteristics retrieved through automated reverse engineering, our CNN model discerns applications as 'botnet' or 'normal' without additional pre-processing or feature selection.

II. LITERATURE SURVEY

The adaptive technique is one of the most prominent ways to increase the performance of the PSO algorithm [2]–[4]. One of the most well-known algorithms introduced in this field (adaptive) is the APSO algorithm [2]. The goal of the APSO algorithm is to improve the efficiency of the PSO algorithm by adjusting the algorithm's primary parameters in response to changes in the search space. This part not only presents the APSO algorithm, but also goes through some of its drawbacks.
In paper [1] they uses deep learning approach using CNN (Convolutional Neural Networks). They tested the approach with 1,929 botnet applications and 4,387 clean apps in large- scale testing. On the same dataset, the model beats many famous machine learning classifiers. The findings show that our suggested CNN-based model can identify new, previously unseen Android botnets more accurately than the other models (Accuracy: 98.9%; Precision: 0.983; Recall: 0.978; F1-score: 0.981
.

III. SYSTEM ARCHITECTURE

Cortes and Vapnik introduced the Support Vector Machine (SVM) [7], a supervised learning model grounded in structural risk minimization and the Vapnik–Chervonenkis dimension. Primarily employed in machine learning, SVMs excel in solving classification or regression problems by identifying the optimal hyperplane to analyze diverse classification data. This optimal hyperplane is characterized by the maximal margin encompassing various classification data points, as illustrated in Figure Two, where two black and three white points lie on the maximal margin line, representing two types of categorization data, commonly referred to as support vectors. SVM discerns and selects extreme points or vectors that constitute the hyperplane, hence termed support vectors, elucidating the nomenclature of this algorithm. While earlier research papers leveraged the CNN algorithm for similar purposes, SVM offers superior accuracy and consistent results.

Explaining SVM through an illustrative example, consider encountering an anomalous feline exhibiting characteristics of a canine. To discern whether the creature is a cat or a dog with precision, an SVM algorithm proves ideal. Initially, the model is trained with a plethora of cat and dog images to grasp their distinguishing features. Subsequently, when confronted with the peculiar creature, SVM delineates a decision boundary between cat and dog data, employing extreme scenarios (support vectors). By discerning the extreme instances of both feline and canine, SVM classifies the creature accordingly. The dimensions of the hyperplane hinge on the dataset's characteristics; for instance, if there are two features, the hyperplane is a straight line, while with three features, it manifests as a 2-dimensional plane.

Furthermore, SVM's support vectors facilitate the classification of new data. In scenarios where data isn't linearly separable, the kernel function maps the data into the Vapnik-Chervonenkis dimensional space to enable effective classification.

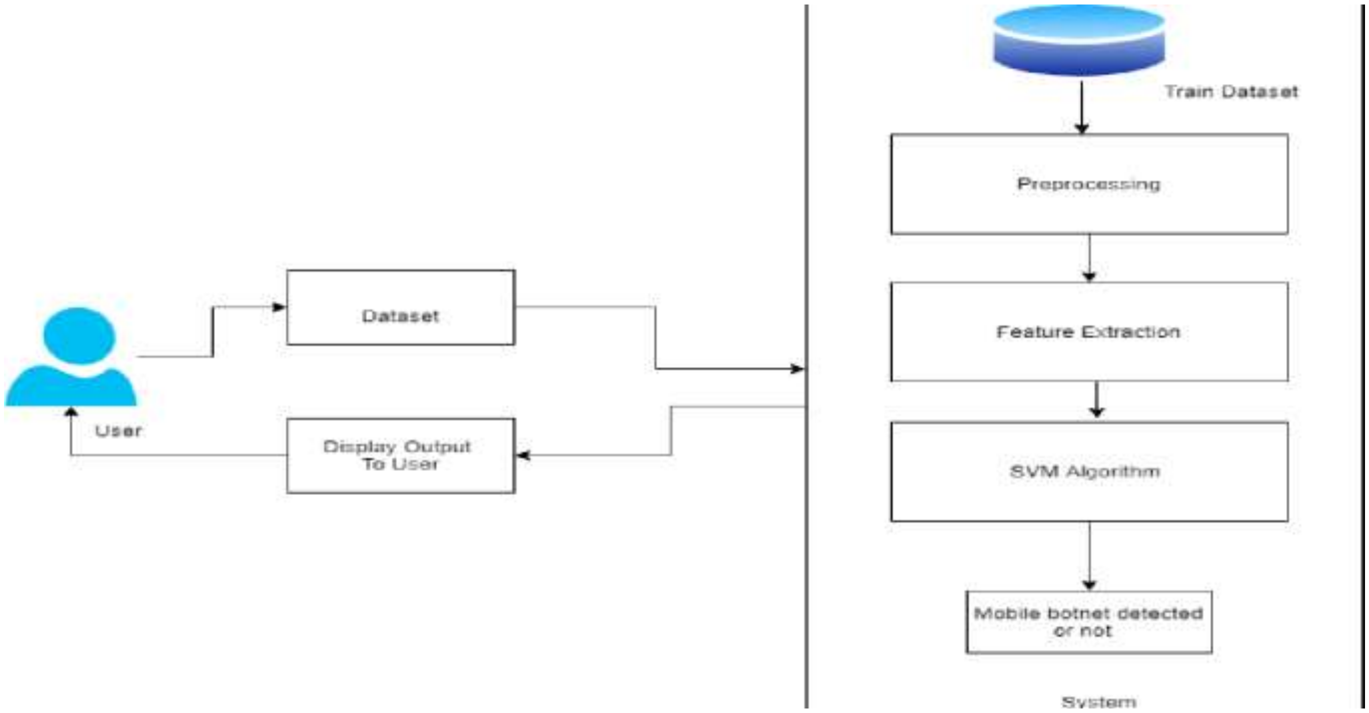

Figure 1. Detail System architecture

Algorithm-:

SVM (Support Vector Machine) [7] is a supervised machine learning technique that may be utilized to solve classification and regression problems. It is, however, usually employed to solve categorization difficulties. Each data item is plotted as a point in an n-dimensional space (where n is the num- ber of features), with the value of each feature being the value of a particular coordinate in the SVM algorithm. Then classification is done by locating the hyper-plane that clearly discriminates the two classes

CONCLUSION

Botnets represent a significant threat within the realm of malware, being utilized for system damage, information theft, and system compromise. Detecting and eradicating them poses a considerable challenge. Hence, our system proves to be a valuable tool for identifying mobile botnets. Looking ahead, there's potential to enhance this model by incorporating additional datasets to improve precision and user-friendliness. These advancements could potentially facilitate its integration into prominent platforms like Playstore and Appstore, although such achievement may not be immediate. Furthermore, its utility extends to local company systems, ensuring the absence of malware across all applications and programs.

REFERENCE

1. Suleiman Y Yerima and Mohammed K Alzaylaee. Mobile botnet detection: A deep learning approach using convolutional neural networks. In 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pages 1–8. IEEE, 2020.

2. Zhi-Hui Zhan, Jun Zhang, Yun Li, and Henry Shu-Hung Chung. Adaptive particle swarm optimization. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 39(6):1362–1381, 2009.
3. Pinkey Chauhan, Kusum Deep, and Millie Pant. Novel inertia weight strategies for particle swarm optimization. Memetic computing, 5(3):229– 251, 2013.
4. Ahmad Nickabadi, Mohammad Mehdi Ebadzadeh, and Reza Safabakhsh. A novel particle swarm optimization algorithm with adaptive inertia weight. Applied soft computing, 11(4):3658–3670, 2011.
5. Yuanyuan Zeng, Kang G Shin, and Xin Hu. Design of sms commanded- and-controlled and p2p-structured mobile botnets. In Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, pages 137–148, 2012.
6. Heloise Pieterse and Martin S Olivier. Android botnets on the rise: Trends and characteristics. In 2012 information security for South Africa, pages 1–5. IEEE, 2012.
7. Tristan Fletcher. Support vector machines explained. Tutorial paper, pages 1–19, 2009.