Sambodhi
(UGC Care Journal)
ISSN: 2249-6661
Vol-43, No.-4, (VI) October-December (2020)

Machine Learning Algorithms to control the security issues in Android Applications

Dr.Sreejith Vignesh B P*
Associate Professor & Head – Information Technology,Sri Krishna Adithya College of Arts and Science, India
Dr.K.Munusamy
Associate Professor & Head – Computer Science,Excel College of Commerce and Science, India

Abstract
The Security issues related to the attacks by hackers and un authorized intruders are prevailing in the world of internet and they are found to be a great headache for the technical advancements especially when dealt with the mobile usage in android application environment. For a new user it is difficult to identify the set of permissions that are harmful. This could be an advantage for malware intruders to access the data or infect the mobile device by introducing malware applications. Thus the face of security has changed in the recent times with the advent of new technologies such as the Cloud, the internet of things, mobile/wireless and wearable technology. The technological advances in data science which help develop contemporary security in networks solutions are storage, computing and behavior. In this paper the possible investigations are done on the cyber attacks in android by adopting the various malware classification and detection techniques. Various Classifications and Detections are done on various malware prevailing in the android applications.
Keywords: Android, Hand held devices, Malware Classifications and Malware Detection Techniques

Introduction

Android and IoS based Smartphones are becoming more popular devices for many people. Due to the rapid entry of smart phones, malware has been spreading widely. An Android OS-based system, being the most popular platform for mobile devices therefore it becomes easy for attackers to target them. Many attackers and hackers take advantage of lack of security standards and limited capabilities in hand held devices. As a result, it paved way for the attackers to steal the personal information of the users of Android mobile devices. From the year 2011, the malware attacks were increased by 155 percent across all platforms. In particular, the hand held devices (using Android OS) is the platform with highest malware growth rate by the end of 2014. Android phones have been sold more than 60% of overall smart phones available Android possessed 82.8% of the market share in 2015 reported in global survey of the OS smart phone market, implying that the growth of the Android is increased when compared to other OS. Today The Android platform is fastest growing market and faces some critical risk.

The swift growth in computer science and information technology in the current times has led to the generation of massive amount of data. As aresult these issues to be considered include optimization, uncertainty quantification, systems theory, statistics and types of model growth. Malware pose significant threats to security in networksof national infrastructures, service sectors, and ultimately the society as a whole. As a result, malware attacks have extended to mobile devices and it has become a necessity to protect ourselves from such attacks. Traditional signature-based and change-based malware detection methods are not able to cope with new types of malware attacks. In order to deal with this problem, in this research project, we plan to develop a practical and effective "anomaly-based" malware detection system with an emphasis on mobile computing platform. We carry out generation of system metrics (i.e., feature vector) and a assortment of efficient machine learning techniques to curtail the malware intrusion in smart devices.

A elemental requirement of hybrid techniques is training and testing on a large dataset, which can lead to improved accuracy. However, existing techniques for machine learning based approaches suffer with low accuracy and high false positive rate (FPR). Also, these techniques have been tested on small datasets. With the emergence of big data [9] and increasing number of malware patterns [4], it is essential that machine learning based malware detection techniques be compared and tested on a large dataset to obtain high accuracy and low FPR. In this paper, we are motivated to improve Android malware detection techniques using big data analytics. Conventional fixed algorithms (hard-wired logic on decision making level) have become ineffective against combating dynamically evolving cyber attacks. This is why we need innovative approaches such as applying methods of applying Machine Learning algorithms and Artificial Intelligence (AI) that provide flexibility and learning capability to software which will assist humans in fighting cyber crimes as AI offers this and various other possibilities. Numerous nature-inspired computing methods of AI (such as Computational Intelligence, Neural Networks, Intelligent Agents, Artificial Immune Systems, Machine Learning, Data Mining, Pattern Recognition, Fuzzy Logic, Heuristics, etc.) have been increasingly playing an important role in cyber crime detection and prevention. AI enables us to design autonomic computing solutions capable of adapting to their context of use, using the methods of self-management, self-tuning, self-configuration, self-diagnosis, and self healing When it comes to the future of information security To this end, we provide a comparison of seven different ML classifiers on the dataset - Using 55 GB dataset and a 19-node Spark cluster, we compared different classifiers including Isotonic Regression, Decision Trees, Random Forest, Gradient Boosted Trees, Support Vector Machine (SVM), Logistic Regression, and Multilayer Perception. We observed that in general, tree based techniques provide better results.

Dr. R. VIMAL NISHANT, M.Com.,M.Phil.,Ph.D.,
PRINCIPAL
Excel College for Commerce and Science
Komarapalayam-637 303.