MJRET

Open Access

Multidisciplinary Journal of Research in Engineering and Technology

Journal homepage: www.mjret.in

ISSN:2348 - 6953

MOBSAFE: ANALYSIS OF ANDROID MOBILE APPLICATIONS USING CLOUD COMPUTING AND DATA MINING

Pranjali Deshmukh, Prof.Pankaj Agarakar
Computer Engineering
DR. D.Y.Patil School of Engineering (Affiliated Affiliated to Savitribai Phule Pune University) Pune, India
pranjali2486@gmail.com,pmagarakar@gmail.com

Abstract: *Android is most popular due to its victim. When upload & download any apk file in android then with there are some of malicious activity are operated with android. However, for gets a security of android application, some proposals are performed. Some technologies are like to using cloud computing and data mining concepts. Mobsafe is the way that performs the methodology regarding with Cloudbroid is a mobile application proposed for cloudStack which provides user friendly interface on a mobile phone. Mobsafe is also gives us faamac i.e. forensic analysis of android mobile applications using cloud computing and K-Means algorithm for selective sort of malevolent android applications. We targeted for achieve mobile application security in android mobile.*

Keywords: *Android platform, mobile malware detection, cloud computing, forensic analysis, machine learning, data mining, **c**loudstack.*

1. INTRODUCTION

1.1 Threats in mobile [1]

Different techniques are follow many users while downloading app in mobile, android provide a easy way for that, but while downloading that automatically brings mobile threats. It also means with this many more techniques are available for detection of malware. There are different ways of android malware origins that are suitable for spreading malwares.

1. First way is to install apps form third party market place.

2. Different market place has different defenses utility.

3. It is easy way to port an existing window based botnet client to android platform.

4. An android application developers are upload their application without checking.

5. A number of applications have been modified and malwares have been packed in and spread.

1.2 Malicious behaviors' of android malware

1. Privilege escalation to root.
2. Leak private data or exfiltrate sensitive data.
3. Dial premium numbers.
4. Botnet activity.
5. Backdoor triggered via SMS.

2. Works related to mobsafe

To achieve security of mobile apps propose a methodology of ASEF & SAAF [1] approximate calculation, time needed to determine all the applications stored in one mobile app to filter out mobile malware.

2.1 Static analysis method

Different researchers perform different analysis methods are analysis based on permission based security model and design some that is self organizing map algorithm provides two-dimensional visualization of high dimensional data and also proposed crowid which uses system calls for finds malware system calls are open( ) , read( ) , access ( ) , chmod ( ) , chown ( ). Next one is presented SAAF provides program. It analyzed 136 000 benign apps and 6100 malicious app.

2.2 Dynamic behavior analysis

In this proposed a methodology paranoid android that is complete malware analysis, also proposed droidMoss which takes fuzzy hashing technique. It used to perform security analysis proposed a methodology paranoid android that is complete malware analysis, also proposed droidMoss which takes fuzzy hashing technique. It used to perform security analysis with technique NFS storage and ZFS file system.

2.3 Work Principle

In mobsafe we not only analyze but also checking security of android apps.

Algorithm:-

1. Submit an apk file to mobsafe

2. Checking the key value store whether the apk file is analyzed & result is stored in hadoop
3. Comparison based on hashing technique of the application file as the key the redis key value store.

4. Redis version is 2.1.3, if the key matched in redis then the output is returned to submitter in the form of response.

5. If the key is unmatched ,it shows a new apk file.

6. After that, it invokes automatize tool such as ASEF & SAAF to collect the logs & store in hadoop directory.

In this technique evaluates the security of android apps.

3. Cloudbroid [2]

It is the application based on android apps & cloud stack, it is an interface between mobile and cloud users. In the cloudbroid the application that manages cloud stack management & which is based on android application using REST Principles. The main idea behind this is accessing the cloud stack system anywhere & anytime with many uses to build an own business opportunity.

3.1 Existing System

There are some problems with this it is more difficult to manage cloud system on mobile & web. Another application that is implemented UI for cloudstack.

3.2 Proposed System

Cloudbriod provides feature like dashboard, storage, template, account, infrastructure, event, project, package & report & also gives easy to read interface than CloudManagerAdvanced. It means we can say that the Cloudbriod overcomes the problem of Cloud Manager Advanced which is not easy to deal or understand management of cloudstack. Cloudstack is platform which contains information as service and also manages, deploys the large number of network virtual machines. In this methodology we can use most popular and useful REST Principle based on java enterprise edition tool or beans. the full meaning of the REST is a Representational State Transfer. REST performs the communication between client & server is in a difficult ways. The protocol is used for the communication HTTP. HTTP has port number eighty.

3.3. System Architecture Overview

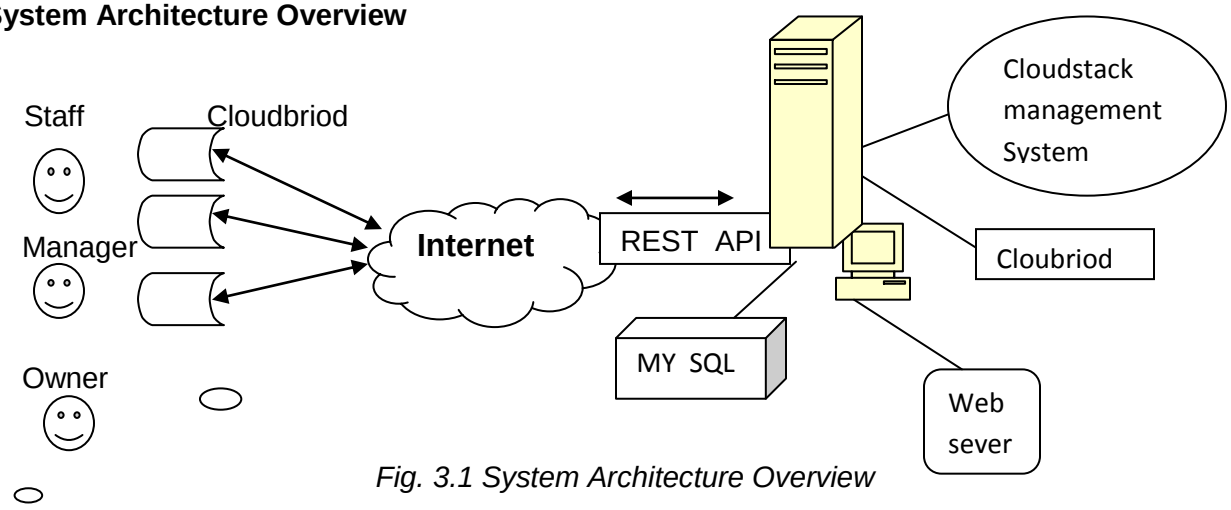

Fig. 3.1 System Architecture Overview

Fig 3.1 shows the system architecture view of cloudstack management and android mobile applications. It consists of mainly two parts; one part is mobile application and cloud stack management. REST API performs the activity of interacts between mobile application and cloud stack management system server. The android mobile application will send the HTTP request to the cloud stack management server. Then, the cloud stack management server will fetch the

information from MySQL database and response back to the user. Cloudbroid implemented in java code on android platform 4.2.2. The application connects with cloudstack server version 4.1.1 by using HTTP Client function in java and the cloudstack API. So the total nine functions that use API command from cloudstack. Some function can only send the HTTP request to retrieve the data but cannot send HTTP POST request.

4. K-Means Algorithm Android Mobile Applications

We can get security by using data mining concepts also k-means[3] and clustering algorithm. Usability and feasibility is increased day by day of mobile apps ,for the purpose , increasing security of mobile apps explain the k-means technique against the malicious activity of android apps.

Most of tread names in android:

1. Andriod.PDaspy
2. Andriod.Opfake
3. Andriod.Obad
4. Driod Dream trojen
5. Android .lucky cat

4.1 K-means

In this mechanism, organize numerical data, or training gets are organized in vectors with a dimension equal to number of features to evaluate.
K means consists of two steps:

1. Calculating the distance from training set vectors to each cluster centroid.
2. Moving the cluster centroid to the means of the respective cluster's members.

4.2 Analysis of clustering algorithm

Clustering algorithm is a process of finds data patterns in huge data. Main aim is the verification of clustering algorithm applied to problem in order highten data set. K-means algorithm uses the permissions of each application as input vectors when performing cluster. Main result of clustering algorithm is that analyze permissions patterns. It means that the distribution of application into different clusters. Distribution of the application means spreads the cluster into different clusters. Density of cluster is means that how the clusters are different.

5. Android Mobile Applications using Cloud Computing

It is verify all mobile apps and to cleanup malware from mobile app market by using cloud computing platform. Mobsafe defines system components & which provides plant from which the system developed.[4].

5.1Steps:-

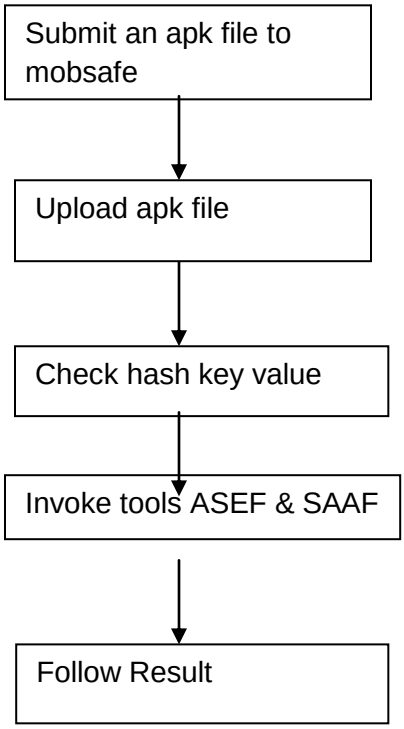

Fig. 5.1 General steps in Mobsafe

ASEF is atomization tool, when upload any file, ASEF performs the activity in three stages. And it launches AVD (Android virtual machine) & install application it. SAAF is a static analyzer for android apk file to analyze permission of apps match discovering patterns.

6. CONCLUSION & FUTURE SCOPE

We can evaluate the security of android apps; we proposed methodology for estimation of analysis and design pattern of android apps. It is well performed on the basis of cloud and data mining. For the purpose, to perform the approximate calculation of active android apps to achieve security. It is proportion of mobile apps popularity, developed mechanism ASEF and SAAF. We also design the cloudbriod to handle android phone application and cloud system make a more easy access anywhere at any time. For future it will be achieve the security of cloud system to expand the applications to be run on any mobile platform. Malwares are also identifying in clusters, so K-Means clustering is suitable in uncovering permission pattern in complete data set and identifying malicious application based on permission request. In future work ,We Will collect huge amount of data, and many apps then use k-means method as well as use neural network technology. This will also helpful for detect the more number of malicious application regarding to android mobile. We also apply the Matrix factorization to check the huge amount of data set. For testing that huge amount of data we also consider the PCA (Primary Component Analysis).

ACKNOWLEGEMENT

My sincere thanks to my guide and our ME Coordinator to Prof. Pankaj Agarakar, for his help and guidance. And I also thankful to our Head of Department Mr.Das and Director Mr.Sonavane sir for giving me this opportunity. I also thankful to all the staff members of the Department of Computer Engineering , Dr.D Y.PATIL(SOE) School of Engineering,Lohegaon Pune for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books.

REFERENCES

[1] Zhen Chen Bin Cao Wenyu Dong Yu Guo Junwei Cao Jianlin Xu, Yifan Yu. Mobsafe: Cloud computing based forensic analysis for massive mobile applications using data mining. TSINGHUA SCIENCE AND TECHNOLOGY, 2013.

[2] Paphawee Lumlert Phapan Niampoonthong Vasaka Visoottiviseth Kantiya Junhom, Sirada Semkham. Cloudbroid: An android mobile application for cloudstack management system. Third ICT International Student ProjectConference, 2014.

[3] Jaykumar Karnewa Snehal Umratkar. K-means algorithm for selective _ltration of malicious android mobile applications. International Journal of Advent Research in Computer , Electronics, 2014.

[4] R.C. Shivamurthy S.V. Nagendra Prasad Yadav. Faamac: Forensic analysis of android mobile applications using cloud computing. International Journal on Recent and Innovation Trends in Computing and Communication, 2014.

[5] Cloudstack project, http://cloudstack.apache.org, June, 2013

[6] CloudStack, A. Understanding Apache CloudStack. 2012 20/11/2013]; Available from: http://cloudstack.apache.org /software.html