International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 3, Issue 5, September-October 2014 **ISSN 2278-6856**

MobShield: Analysis for Mobile Applications using Cloud Computing with Data Mining

Ms. Puja S.Tekade[1], Prof. Arvind S. Kapse[2]

[1]M.E.Second Year CSE, P. R. Patil COE&T, SGBAU, Amravati, Maharashtra ,INDIA

[2] Assistant Professor, Dept. of CSE, P. R. Patil COE&T, SGBAU, Amravati, Maharashtra, INDIA

Abstract

With day to day increase in the number of mobile applications there is an analogous increment in the mobile threats. For such kinds of threats to mobile devices there should be some security mechanism to be implemented . In this proposed system in order to improve the security to the mobile apps one methodology is proposed which will evaluate the mobile applications based on the cloud computing platform and data mining. Here also a prototype system named MobShield is presented to identify the mobile app's virulence or benignancy. Compared with traditional method, such as permission pattern based method, MobShield combines the dynamic and static analysis methods to comprehensively evaluate an Android app. In the implementation, Android Security Evaluation Framework (ASEF) and Static Android Analysis Framework (SAAF) are adopted , the two representative dynamic and static analysis methods, to evaluate the Android apps and estimate the total time needed to evaluate all the apps stored in one mobile app market. As mobile app market serves as the main line of defense against mobile malwares, the evaluation results show that it is practical to use cloud computing platform and data mining to verify all stored apps routinely to filter out malware apps from mobile app markets. In this proposed system the concept will be extended with the implementation of K-means algorithm.

Keywords:- Android platform; mobile malware detection; cloud computing; forensic analysis; machine learning; data mining.

1. Introduction

Technology is changing everyday. Now the phone is being turned into smartphones.[1]In past times the phone is used only to facilitate the communication between people .The additional facilities included SMS and browsing facilities . Now the technology is changed and mobile phones comes with android and windows operating systems. With android operating system lot of applications are provided for users to manipulate all types of data. The user is being provided with all types of applications for entertainment , travelling , communication, browsing, music , pictorization and lot more. With that much increase in technology access strategies are increased and security issues are arised.[3]with multiple app markets we blindly download lot of apps in our mobiles but because of malwares and viruses such apps may harm the security of our mobiles. By those malwares security of important mobile data is threatened.To provide security to mobile data various security applications are being propsed. Here in this work also a methodology is being proposed to provide security to mobiles.Here security mechanism include cloud computing and data mining.

2. Literature Servey

Jianlin Xu, Yifan Yu, Zhen Chen have proposed a system which has combination of dynamic and static frameworks to provide security to commertial mobile applications [4]. They have analysed the amount of time needed to indicate and find out the non secure applications among the installed apps [5]. Barrera et al.[6] made an analysis on permissionbased security models and its applications to Android through a novel methodology which applies Self-Organizing Map (SOM) algorithm preserving proximity relationships to present a simplified, relational view of a greatly complex dataset. The SOM algorithm provides a 2-dimensional visualization of the high dimensional data, and the analysis behind SOM can identify correlation between permissions[6]. Enck et al.[7] (TaintDroid) built a tool that warns users about applications that request blacklisted sets of permissions. They took both dangerous functionality and vulnerabilities into consideration and applied a wide range of analysis techniques[7]. They have just analysed appchina commertial application market and given the time analysis of identifying the bug free apps for secure use.In their work they only did time analysis [6]. But in the current work instead of doing time analysis the application notifies about the theft [7].

3. Proposed Work

In this work a methodology is being proposed which provides security to your mobile phone from malwares that comes from faulty apps.

It includes following:

1. It includes combination of dynamic and static methods to provide security.
2. It includes data mining techniques.
3. It includes some method that is used to provide optimized outputs.
4. It will include the checkpoints of the database that will indicate the safe state of database and that backup will be used to restore the database in case of failures.
5. It will use the database which will be the combination of five tables to store the various types of data having contact details, sms and other information.
6. In case of database failures the location of the device will be detected with the help of checkpoints.

Following flowchart shows the complete procedure of Mobshield:

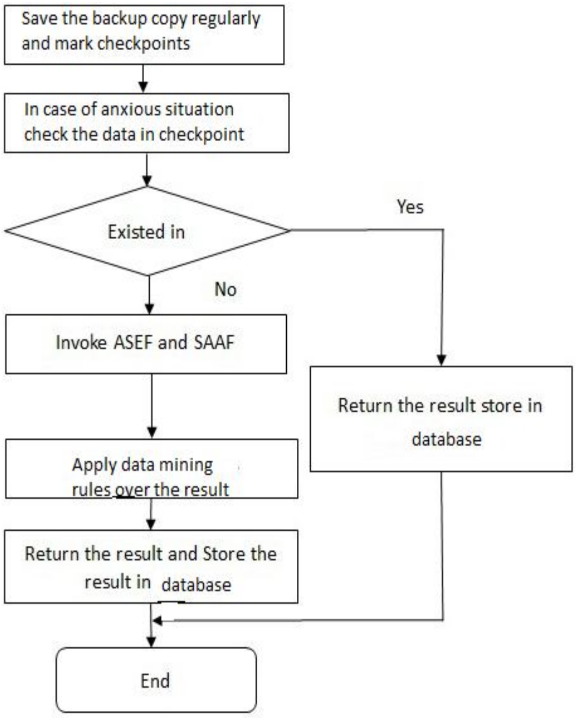
Save the backup copy regularly and mark checkpoints
In case of anxious situation check the data in checkpoint
Existed in
Yes
No
Invoke ASEF and SAAF
Return the result store in database
Apply data mining rules over the result
Return the result and Store the result in database
End

Fig. 1 : The Procedure of analysis of mobile apps in Mobshield

This will include six modules which are as follows:

1. The database creation of having six tables.
2. Development of mobile application for parameter tracking.
3. Establishing the communication between the cloud and the mobile.
4. Development of data mining techniques.
5. Forensic analysis on data.
6. Result analysis and data optimization.

4. Conclusion

By this methodology massive data can be protected from malwares and the database can be protected. The prototype system Mob Safe can be implemented for automation forensic analysis of mobile apps static code and dynamical behavior ASEF(Android Security Evaluation Framework) and SAAF(Static Android Evaluation Framework) the two representative dynamic analysis method and static analysis method can be used to evaluate the Android apps and estimate the total time needed to evaluate all the apps stored in a mobile app market .

5 Future Work

As the future perspective some web mining and more advanced data mining techniques will be implemented to get more optimized outputs. Machine learning is the issue which will be in the future work of this system. As we collect more and more app' slogging and network behavior data, we can further use K-means method to classify apps and to distribute the database. In this case, the accuracy metrics includes precision and recall can be measured to evaluate the classifier algorithm. Other method such as PCA (Primary Component Analysis) and Matrix Factorization also can be used and tested on such data in order to provide more accuracy.

References

[1] R. Lawler, Mary Meeker's 2013 Internet Trends report, http://techcrunch.com/2013/05/29/mary-meeker-2013- internet-trends/, September 2, 2014.

[2] Jianlin Xu, Yifan Yu, Zhen Chen_, Bin Cao, Wenyu Dong, Yu Guo, and Junwei Cao, "MobShield: Cloud Computing Based Forensic Analysis for Massive Mobile Applications Using Data Mining", TSINGHUA SCIENCE AND TECHNOLOGY ISSN 1007-0214 10/10, pp. 418-427 ,Volume 18, Number 4, August 2013.

[3] Gartner,http://www.gartner.com/it/page.jsp?id=2153215,September 3, 2014.

[4] List of mobile software distribution platforms,http://en.wikipedia.org/wiki/List of digital distribution platforms for mobile devices, July 19, 2013.

[5] D. Barrera, H. G. Kayacik, P. C. van Oorschot, and A. Somayaji, "A methodology for empirical analysis of permission-based security models and its application to Android, in Proc.", 17th ACM Conference on Computer and Communications Security, Chicago, USA, 2010, pp. 73-84.

[6] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, "Android permissions demystified", in Proc. 18th ACM Conference on Computer and Communications Security, Chicago, USA, 2011, pp. 627-638.

[7] K. O. Elish, D. Yao, and B. G. Ryder, "User-centric dependence analysis for identifying malicious mobile apps", in Workshop on Mobile Security Technologies (MoST), San Francisco, USA, 2012