International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 06 | June-2018 www.irjet.net p-ISSN: 2395-0072

Monitoring and Detecting Abnormal Behaviour in Mobile Cloud Infrastructure

Patil Supriya Gulabrao[1], Salunkhe Anumita Vijay[2], Pawar Arati Mansing[3], Patil Prachi Rajiv[4], Ms. Khambalkar Chhaya Hanamant[5]

Asst. Prof. AITRC, Vita, Maharashtra , India.

Abstract - *several mobile Devices and it's services are changing to cloud-based mobile services with richer communications and higher flexibility. We present a new mobile cloud infrastructure that combines mobile devices and cloud services and Database Services. This new infrastructure provides virtual mobile instances through cloud computing. To commercialize new services with this infrastructure, service providers should be aware of security issues. In this paper, we first define new mobile cloud services and Database service through mobile cloud infrastructure and discuss possible security threats through the use of several service scenarios. Then We Propose Architecture for detecting abnormal behavior. To Test Our Methodology we use machine learning technique.*

Key Words: (Size 10 & Bold) Key word1, Key word2, Key word3, etc (Minimum 5 to 8 key words)…

INTRODUCTION

In line with the numerous electronics manufacturers producing new mobile devices such as smart phones and smart tablets, various mobile services are being provided as applications for these devices. There are more than 200,000 Android and 300,000 iPhone applications available as of March 2011 and these numbers are increasing rapidly. One recent trend for mobile services is their change to cloud-based mobile services. Cloud-based mobile services benefit users by richer communications and higher flexibility. Richer communications mean advanced techniques supporting such as enhanced phonebooks, messaging with push notification, and enriched call with multi-media content sharing. Massive computational processing is performed through cloud computing infrastructure instead of low-speed mobile devices. The data stored in cloud infrastructure can be accessed at any running text should match with the list of references at the end of the paper.

time and from anywhere through mobile devices. As a result, richer communications and higher flexibility can be provided to mobile device users through cloud computing. Through the convergence of mobile devices and cloud services, we expect that new mobile cloud services will be provided with the virtualization of mobile devices in cloud infrastructure. Virtual smart phone over IP is one example of provisioning virtual mobile instances to users. Each virtual instance in cloud infrastructure represents a mobile device, and users can connect to and use this instance. In this paper, we present a mobile cloud infrastructure as an infrastructure that provides virtual mobile instances, and those instances are managed in cloud computing architecture with massive computational processing power and storage.

However, service providers should be aware of security problems that may arise when they adopt and launch new cloud services. According to an IDC report, when questioned, 74.6% of service providers answered that the most important issue for cloud services is security. In addition, recent cloud computing attacks make it difficult to guarantee the trust and safety of cloud services. For mobile cloud services, malicious mobile applications can be run on virtual mobile instances and therefore any security problems may be much severe if those applications target on the virtualization of mobile cloud infrastructure.

1.1 APPLICATION IN GENERAL FORM IN DIFFERENTAREAS

Mobile Devices and services are changing to cloud-based mobile services with richer communications and higher flexibility. We present a new mobile cloud infrastructure that combines mobile devices and cloud services. This new infrastructure provides virtual mobile instances through cloud computing. To commercialize new services with this infrastructure, service providers should be aware of security issues.

We first define new mobile cloud services through mobile cloud infrastructure and Database Services. Then We Propose Architecture for detecting abnormal behavior. To Test our technique we will use machine learning algorithms. Our System having the direct communication between the company and the students or the applicants with the help of the cloud which going to act as middleware for them. Cloud based system is again introduced with the recognition of the abnormal behavior.

As we know, now days such tasks are handled by the consultancy companies which again uses the paid services strategy. The system focuses on the abnormal behavior detection in mobile cloud infrastructure. It is difficult for users to install Specific Software to detect the behavior of users. Behavior based abnormal detection can address the activities of users in the cloud infrastructure. To achieve this, we design a monitoring architecture using both the host and network data and Database Services. Using Analyzed Data we apply the machine learning algorithm to detect the behavior of users

1.2 CHALLENGES IN EXISTING SYSTEM

Many systems are presently working on the same problem and they even providing the solution on their way. Existing systems are not cloud based and therefore they are not able to provide the solution in the efficient behavior. The systems present existing are not able to provide client to client service. They are taking users data on their site which is not good way and even users are not being sure about safety of their data. Even the existing systems are not providing end to end security to the user's data. On such normal mobile devices, most current vaccine applications detect malware through a signature-based method. Signature-based methods can detect malware in a short space of time high accuracy, from only the known database. So vaccine applications cannot detect and prohibit malware with only signature-based method. Mobile cloud infrastructure supports a large number of virtual mobile instances. When a malware is compromised on a virtual mobile instance, it can be delivered to other virtual mobile instances in the same mobile cloud infrastructure. Without monitoring the network behavior in mobile cloud infrastructure, the malware will spread over the entire infrastructure.

2. PROPOSED SYSTEM

Our Main Aim is to detect the Abnormal behavior of users in the cloud infrastructure. Although signature-based vaccine applications can target on virtual mobile instances to detect malware, it makes additional overhead on instances, and it is difficult for users to install vaccine software by force.

For this we will use the Random Forest Algorithm

3. SYSTEM ARCHITECTURE

Random Forest is an ensemble learning based classification and regression technique. It is one of the commonly used predictive modeling and machine learning technique.

The random forests algorithm (for both classification and regression) is as follows:

1. Draw ntree bootstrap samples from the original data.

2. For each of the bootstrap samples, grow an unpruned classification or regression tree, with the following modification: at each node, rather than choosing the best split among all predictors, randomly sample mtry of the predictors and choose the best split from among those variables. (Bagging can be thought of as the special case of random forests obtained when

mtry = p, the number of predictors.)

3. Predict new data by aggregating the predictions of the ntree trees (i.e., majority votes for classification, average for regression).

4. CONCLUSION

In this paper, we presented a new mobile cloud service with the virtualization of mobile devices and discussed some possible scenarios for individual users and office workers. To address security issues in mobile cloud infrastructure, we proposed abnormal behavior monitoring methodology and architecture to detect malware. These were then tested by deploying our mobile cloud test bed. Host and network data are used together to detect abnormal behavior. Our abnormal behavior detection using the Random Forest machine learning algorithm.

5. REFERENCES

[1] [1] F. Gens, "IT Cloud Services User Survey, pt.

[2] 2: Top Benefits & Challenges", IDC exchange (http://blogs.idc.com/ie/), August 14, 2008.

[3] Y. Chen, V. Paxson, and R. H. Katz, "What's New About Cloud Computing Security," University of California Berkeley Report No. UCB/EECS-2010-5, January 2010.

[4] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications 2010, Vol.34, No.1, July 2010, pp.1-11.

[5] A.Shabtai, U. Kanonov, and Y.Elovici, "Andromaly: a behavioral malware detection framework for android devices", Journal of Intelligent Information Systems, January 2011, pp 130.

[6] D.Damopoulos, S.A. Menesidou, G. Kambourakis, M. Papadaki, N. Clarke, and S. Grizali, "Evaluation of Anomaly-Based IDS for Mobile Devices Using Machine Learning Classifier", Security and Communication Networks, Vol.5, No.1, January 2011, pp.3-14.

[7] W. Enck, P. Gilbert, B. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones", In Proc. of the USENIX Symposium on Operating Systems Design and Implementation (OSDI), Vancouver, Canada, October. 4-6, 2010.