A Cloud based Solution for Abnormal Behavior using RF Algorithm in Mobile Environment

M. Arun prakash and Rabiyathul basariya

Abstract: Mobile cloud computing is an emerging technology.it is the combination of mobile devices and cloud services. It is called a mobile cloud infrastructure. This infrastructure provides the virtual mobile instances through cloud computing. In this paper we are using the machine learning algorithm. It is used to detect the abnormal behavior in mobile cloud infrastructure and also using methodology and architecture for detecting abnormal behavior through the monitoring of both host and network data. To the Random Forest (RF) machine learning algorithm to detect the abnormal behavior that arose from these programs.

Keywords: Mobile Cloud Infrastructure, Mobile Cloud Computing and Service Scenarios, Monitoring Abnormal Behavior, RF Machine learning.

I. INTRODUCTION

One of the recent trends for mobile services is the cloud – based mobile services. The cloud-based mobile services benefits are richer communication with users and higher flexibility. Richer communication means to support the advanced techniques, such as enhanced phonebooks, messaging with push notification, and enriched call with multi-media content sharing. The data's are stored in cloud infrastructure.

Using the mobile devices we can access the data at anytime and anywhere finally the mobile cloud infrastructure provide the richer communications and higher flexibility to mobile device users. Massive computational processing is performed through cloud computing infrastructure. The mobile cloud services to provide the virtualization of mobile devices in cloud infrastructure. Virtual smartphone is one example of virtual mobile instances to users.

In cloud computing, service providers should be aware of security problems that may arise when they adopt and launch new cloud services. Nowadays normal mobile devices using the vaccine application to detect the malware through a signature based method, it detects malware in a short period of time with high accuracy, but they cannot detect new malware this signature is unknown or has been modified. Therefore vaccine applications cannot detect and prohibit them with only signature-based method in the future. 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. if the network has without monitoring the malware will appear spread over the entire infrastructure. Although signature-based vaccine applications can target on virtual mobile instances to detect malware, it makes additional overhead on instances. But it is difficult for users to install vaccine software.

M.ArunPrakash, RabiathulBasariya is with SOC/Sastra University.
Emails: arunit@it.sastra.edu, basariya@cse.sastra.edu

In this paper, introduce the **Monitoring architecture and Random Forest (RF) machine learning algorithm.** We have to design a monitoring architecture using both the host and network data and to use the machine learning algorithm to detect the abnormal behavior in mobile cloud infrastructure. To validate our methodology, we built a test bed for mobile cloud Infrastructure. To install malicious mobile programs onto several virtual mobile instances, and then successfully detected the abnormal behavior that arose from those malicious programs.

II. PROBLEM STATEMENT

Vaccine applications detect malware through a signature-based method. Signature-based methods can detect malware in a short space of time with high accuracy, but they cannot detect new malware whose signature is unknown or has been modified.

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.

III. RELATED WORKS

A. Monitoring Abnormal Behavior in Mobile Devices

B. Abnormal Behavior in Cloud Computing Infrastructure

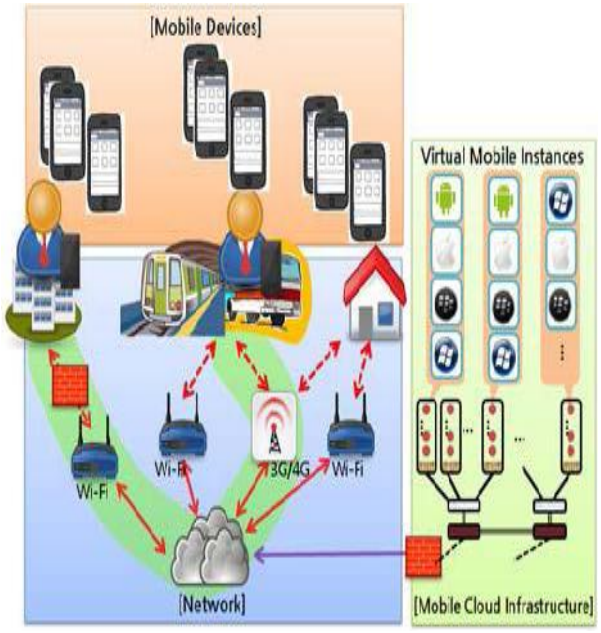
Several research groups have targeted intrusion detection for cloud computing infrastructure and monitoring architecture and requirements that can detect the malicious behavior in cloud infrastructure. They identified Intrusion Detection System (IDS) management issues in the cloud considering both Host IDS (HIDS) and Network IDS (NIDS). In their architecture, they performed behavior analysis with the collaboration of each node, and also used knowledge-based analysis. This architecture does not reflect virtualization of each node when virtual instances are provided to users through cloud computing infrastructure.

Mobile Cloud Service and Scenarios

There are two main service scenarios to explain how this mobile cloud service can be used. Service scenarios are useful to security threats on mobile cloud infrastructure, because they include users, places, mobile devices, and network types, and user's interesting contents.

Defining Mobile Cloud Computing and the Concept of Mobile Cloud Service

Mobile Cloud Computing means assign large role to mobile devices for cloud computing. For example, *Warner et al.* defined mobile cloud computing as accessing the cloud through mobile devices and also mobile devices becoming part of a larger cloud construct. *Marinelli* referred to mobile cloud computing as a term meaning that a number of mobile devices construct a cloud computing group, and jobs are allocated to various device nodes in order to execute computing jobs faster. The mobile cloud computing as processing jobs for mobile devices in cloud computing infrastructure and delivering job results to mobile devices.
The proposed mobile cloud service provides virtual mobile instances through the combination of a mobile environment and cloud computing. Virtual mobile instances are available on mobile devices by accessing the mobile cloud infrastructure. This means that users connect to virtual mobile instances with their mobile devices and then use computing resources such as CPU, memory, and network resources on mobile cloud infrastructure. By mobile cloud services, any mobile devices can be a super computer and they can support several rich services.



Service Scenarios for Mobile Cloud Services

Security threats to our mobile cloud service depend on how the service is prepared and delivered from the service providers
to the actual users. The possible service scenarios on our mobile cloud service into two main categories.

1. Individual users
2. Office workers

1. Individual users

Individual users use the mobile cloud service for entertainment and other individual purposes. Individual users are categorized as normal users, advanced users and developers according to usage types and their requirements.

A. Normal Users:

These users are more interested in the services available from the mobile cloud environment
Than environment itself. The cloud environment required by these users.

B. Advanced Users:

These users are know the awareness of overall mobile cloud services and more interested in cloud resources than normal users. They also require a cloud environment that varies more frequently.

C. Developers:

These users are aware of overall mobile cloud services and require a cloud environment that is specific, varied and which changes frequently.

***2)* Office workers**

Office workers are categorized as staff in a main office, staff in overseas offices and subcontractors according to their office location and relationship to the company.

A. Staff in a main office:

These users work on mobile office systems installed in the main office.

B. Staff in overseas offices:

These users access mobile office systems from overseas offices to the main office. The network condition in foreign countries may be poorer than domestically accessed mobile offices. Therefore these users are interested in a stable mobile office environment.

C. Subcontractors:

These users contract as developers of the main office, co-work or run a project together with the company. If their contract is no longer valid, subcontractors should not use mobile office systems provided from the main office.

Algorithm Implementation

We used the Random Forest (RF) machine learning algorithm to detect the behavior with our collected data which is present on the mobile cloud services applied on the infrastructure. The RF algorithm is a combination of decision trees that each tree depends on the values of a random vector sampled independently and with the same distribution for all trees in the forest. We represented the collected features as a vector with the data subsequently used to train our collected data set. This algorithm was introduced by Breiman which describes about the many random classification of trees.

IV.CONCLUSION

In this paper ,we discussed a new mobile cloud service with the virtualization of mobile devices and some possible scenarios for individual users and office workers and use monitoring architecture and machine learning

algorithm to detecting the abnormal behavior in mobile cloud infrastructure. Monitoring algorithm used to detect the 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 RF machine learning algorithm successfully detects abnormal behavior.

IV. FUTURE WORK

The monitoring of mobile cloud infrastructure focusing on security issues, other monitoring metrics should be considered for the provisioning and configuration, of services, and for the charging of users. To measures the performance of our proposed monitoring architecture, deal with the security aspects of this service and various additional types of malwares to improve the accuracy of using various machine learning algorithms. Further, we will consider other monitoring features to improve the accuracy of detecting abnormal behavior. But there is an overhead issue such as time complexity and battery consumption if we gather lots of features.

REFERENCES

[1] C. Dwork, “The Differential Privacy Frontier Extended Abstract,” Proc. 6th Theory of Cryptography, Springer, 2009.

[2] White, Mark “Machine Learning-lecture Slides, Fall 2005.

[3] E. Naone, “The Slow-Motion Internet,” Technology Rev.Apr. 2011;

[4] I. Burguera, U. Zurutuza and S. Nadjm- Tehrani, "Crowdroid: Behaviorbased malware detection system for android", Proceedings of the 1st workshop on Security and privacy in smartphones and mobile devices(SPSM’11), New York, NY, USA, October 17, 2011.

[5] E. E. Marinelli, "Hyrax: cloud computing on mobile devices using MapRecuce", a Mater Thesis, CMU-CS-09-164, Carnegie Mellon University, September, 2009 which is available in Url:http://reportsarchive.adm.cs.cmu.edu/anon/2009/CMU-CS-09-164.pdf.

[6] 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.

[7] A.Shabtai, U. Kanonov, and Y.Elovici, "Andromaly: a behavioral malware detection framework for android devices", Journal of Intelligent Information Systems, January 2011, pp 1-30.

[8] 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.

[9] 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.

[10] I. Burguera, U. Zurutuza and S. Nadjm-Tehrani, "Crowdroid: behaviorbased malware detection system for android", Proceedings of the 1st workshop on Security and privacy in smartphones and mobile devices (SPSM’11), New York, NY, USA, October 17, 2011.

[11] E. E. Marinelli, "Hyrax: cloud computing on mobile devices using MapRecuce", a Mater Thesis, CMU-CS-09-164, Carnegie Mellon University, September, 2009, available on http://reportsarchive.adm.cs.cmu.edu/anon/2009/CMU-CS-09-164.pdf.

[12] S. A. Warner and A. F. Karman, "Defining the Mobile Cloud", NASA IT Summit 2010, August 16-18, 2010.

[13] GoldMiner, http:// blog. mylookout. Com / blog/ 2010/ 12/29/geinimi_trojan/, December 2010.