ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

National Conference on Innovative Applications and Research in Computer Science and Engineering (NCIARCSE-2017)

AGTI's Dr. Daulatrao Aher College Engineering, Vidyanagar Extension, Karad

Vol. 4, Special Issue 4, January 2017

Abnormal Behaviour Detection using Mobile Cloud Infrastructure

Prof. Sumalatha D. Bandari[1], Sana I. Mulla[2]

Professor, Computer Science & Engg, DACOE, Karad, India [1]

Student, Computer Science & Engg, DACOE, Karad, India [2]

Abstract: Now days, some mobile services are changed with cloud-based mobile services with richer communication and greater flexibility. So, we now present new mobile cloud infrastructure with including features of mobile devices and cloud services. With cloud computing this infrastructure provides the virtual mobile instance. For commercialize new services, service providers should be aware from security obstacles. Hence we introduce new mobile cloud services with mobile cloud infrastructure and defines possible security problems with use of some service scenario. Hence, we introduce methodology and architecture for detecting abnormal behavior through the monitoring of host and network data. To validate our methodology, we used machine learning algorithm to detect the abnormal behavior that arose from these programs.

Keywords: Mobile devices, Random Forest Machine Learning algorithm, Abnormal Behaviour.

INTRODUCTION

In normal mobile devices, most current vaccine applications detect malware through a signature-based method. Signature-based methods can detect malware in a short period of time with great accuracy, but they cannot detect new malware whose signature is unknown or has been modified. If mobile cloud services are provided, there may be possibility of malicious applications may appear including new and modified malware.[1]

Vaccine applications cannot detect with only signature-based method in the future. Moreover, mobile cloud infrastructure supports a maximum 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 behaviour in mobile cloud infrastructure, the malware will spread over the entire infrastructure.
The cloud infrastructure is vulnerable if specific security measures are not implemented.

RELATED WORK

Mobile devices with cloud based services are very effective. Mobile cloud infrastructure is recently introduced where mobile devices and cloud services are combined together. As it a commodity, service providers should know the security issues.

In various security threats are mostly discussed based on its situation. A new methodology is introduced in order to detect the abnormal behavior. By detecting the host and the communicating devices certain malicious programs are injected in the test bed to identify the abnormal behavior. Using machine learning algorithm, these suspicious programs are detected. For finding the next neighboring node and to detect the fault, FDMC algorithm is implemented.

Algorithm Implementation

This 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

The random classification contains the dataset that is formed by combining with position replacement in the training set. In our proposed system, we used malware detection for the applications it describe about the security threats for the existing system and applications on mobile cloud instances. It create based on the malicious software that is installed on the mobile cloud services. In our proposed system we detect the normal behaviour by introducing signature based method. But this method is not applied for modified cloud instances and new malware which is unknown for the cloud service scenarios explained about the mobile cloud services i.e. vaccine applications so it is better to causes on future proposals. If malware is present on the cloud instance then it is applied on other mobile cloud service provider which is present on the similar host and it also useful for detecting malicious programs and the abnormal data to be monitored through

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
National Conference on Innovative Applications and Research in Computer Science and Engineering (NCIARCSE-2017)
AGTI's Dr. Daulatrao Aher College Engineering, Vidyanagar Extension, Karad
Vol. 4, Special Issue 4, January 2017

some usage and enhance for future applications. The main analysis is taken for each mobile cloud instance over virtual applications.[3]

PROPOSED APPROACH

Here we propose how to identify and detect security threats in Mobile Cloud Infrastructure. Here, we discuss some possible security threats to Mobile Cloud by way of illustrative service scenarios that involve both individual users and office staff. As a feasible solution of detecting the identified security threats, we propose a behavior-based abnormal detection methodology of monitoring both virtual hosts and network data. Here we show that our solution is better able to detect new, modified, and unknown abnormal activities than signature-based methods. So the detection methodology is based on a machine learning technique, which uses both training (on normal and abnormal mobile applications) and monitoring real-time traffic. In our testing, our solution successfully detected the abnormal activities of malicious behavior, which were intentionally injected into a mobile cloud test bed. With the Help of Cloud Infrastructure our Problem Definition is develop an Android App to detect the Suspicious Behaviors of Users.

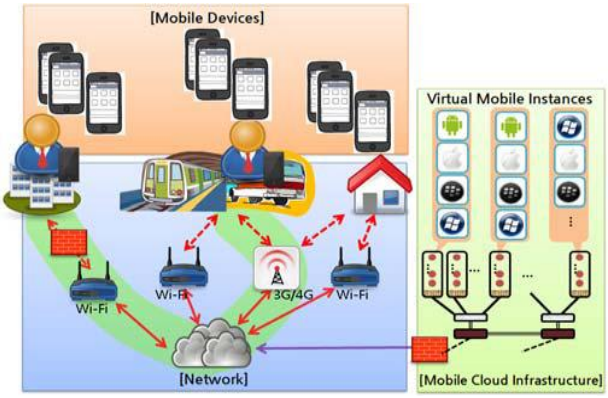

Fig. 1. The Concept behind our Defined Mobile Cloud Service

1. User Account
2. Mobile Cloud Service
3. Malware Data
4. Abnormal Behavior Detection

1. User Account

In this module, Users are having authentication and security to access the details which are presented in the system. Before accessing or searching the details from system user should have the account in that system otherwise they should register first.

2. Mobile Cloud Service

Here new mobile cloud services presented through the virtualization of mobile devices in cloud infrastructure. Here, we describe two main service scenarios to explain how this mobile cloud service can be used. Service scenarios are useful to describe security threats on mobile cloud infrastructure, because they contains users, mobile devices, and network types, and user's interesting contents.

Now, we define mobile cloud computing as processing jobs for mobile devices in cloud computing infrastructure and giving job results to mobile devices. we expose a new mobile cloud service as providing virtual mobile instances by using mobile cloud computing. The proposed mobile cloud service provides virtual mobile instances through both of a mobile environment and cloud computing. The virtual mobile instances are available on mobile devices by accessing the mobile cloud infrastructure. Here users are connected to virtual mobile instances with their mobile devices and then use computing resources like CPU, memory, and network resources on mobile cloud infrastructure. In this case, these mobile devices will have smaller roles to play than current mobile devices.

3. Malware Data

We installed the malware onto two hosts and run it. It gathers location coordinate and device identifiers (IMEI and IMSI), and sends the information to its server. The malware target is to affect each mobile instance as zombie, and there are many other malware which have the same purpose although their functionality and behavior are little different from each other. This kind of malware is more affecting to mobile cloud infrastructure because there are lots of similar virtual mobile instances and they are closely connected to each other. If entered data are not same as compare to the data in database that is called as malware data.

4. Abnormal Behavior Detection.

Here we use Random Forest (RF) machine learning algorithm to train abnormal behavior with our collected data set. The RF algorithm is a combination of decision trees in which each tree depends on the values of a random vector, sampled individually with the same distribution for all trees in the forest. We represented the collected features as a vector with data subsequently used to train our Derived data set.

CONCLUSION

In our paper, we presented a new mobile cloud service with the virtualization of various mobile devices and discussed some possible scenarios for individual users and office workers. To address security issues in mobile cloud infrastructure, we proposed abnormal behaviour 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 behaviour. Our abnormal behaviour detection using the RF machine learning algorithm shows that our proposed methodology and architecture successfully detect abnormal behaviour.

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

National Conference on Innovative Applications and Research in Computer Science and Engineering (NCIARCSE-2017)

AGTI's Dr. Daulatrao Aher College Engineering, Vidyanagar Extension, Karad

Vol. 4, Special Issue 4, January 2017

REFERENCES

[1] "Monitoring and Detecting Abnormal Behaviour in Mobile Cloud Infrastructure",Taehyun Kim, Yeongrak Choi, Seunghee Han, Jae Yoon Chung,Jonghwan Hyun, Jian Li, and James Won-Ki Hong.

[2] "A Cloud based Solution for Abnormal Behaviour using RF Algorithm in Mobile Environment", M. Arun Prakash and Rabiyathul basariya.

[3] "Providing Cloud Services Over Mobile Cloud Data", Sruthi Tammana, Sri Rashmi Matta, Dr.S.Satyanarayana.

BIOGRAPHIES

Sana I. Mulla is perceiving BE from AGTI's Dr. Daulatrao Aher College of Engineering, Karad, India. Her area of interest Cloud computing.

Sumalatha D. Bandari received Diploma in Electronics & Telecommunication Engineering from Government Polytechnic for Women, Nizamabad, Andhrapradesh in 2001. B. Tech degree from Jawaharlal Nehru Technological University, Hyderabad in Computer Science & Information Technology in 2005, the M. Tech degree from Jawaharlal Nehru Technological University, Hyderabad in 2011. From 2006 to 2010 she worked as an Assistant Professor in Department of Information Technology of Indur Institute of Engineering & Technology, Siddipet, Andhrapradesh. From 2011 to May 2012 she worked as an Assistant Professor in Department of Computer Science & Engineering of Rajarambapu Institute of Technology, Sakharale, District Sangli, Maharashtra. Since June 2012 she is working as an Assistant Professor in Information Technology Department of Dr.Daulatrao Aher College of Engineering, Karad, District Satara, Maharashtra. Her area of interest includes Natural language Processing, Machine Learning & Cloud Computing.