Random Forest (RF) Machine Learning Algorithm to Detect Abnormal Behavior in Cloud – Based Mobile Services

Supraja.Y#[1], T.V.Sai Krishna#[2], P.VenkataSubbaReddy#3, Dr.M.A.D.Swamy#4,Dr.P.Srinivasulu #5

Student, Department of CSE, QIS College of Engineering and Technology, Ongole, India#[1]

Associate Professor, Department of CSE, QIS College of Engineering and Technology, Ongole, India#[2]

Associate Professor, Department of CSE, QIS College of Engineering and Technology, Ongole, India#[3]

Professor, Department of CSE, QIS College of Engineering and Technology, Ongole, India#[4]

Professor, Department of CSE, QIS College of Engineering and Technology, Ongole, India#[5]

Abstract--Cloud computing has become a realized computing phenomenon. In fact it is the new way of computing in which systems operate. Now mobile devices also can participate in cloud computing. Mobile services are being moved to cloud as the cloud provides plethora of benefits to users of mobile computing and also the service providers. Recently,Kim et al. presented a new mobile cloud infrastructure for combining both cloud services and cloud devices. The infrastructure enables virtual mobile instances as part of cloud computing. This new infrastructure can be used by service providers. However, they should be aware of issues pertaining to security. They discussed various security problems and solutions with respect to mobile cloud infrastructure. The main aim was to monitor and detect abnormal behavior in mobile cloud infrastructure. In this paper we implement this concept practically. We built a prototype application, a custom simulator that demonstrates the proof of concept. The empirical results revealed that the proposed approach can detect abnormal behavior in mobile cloud infrastructure.

Index Terms –Cloud computing, mobile infrastructure cloud, cloud service providers

I. INTRODUCTION

Mobile devices are being manufactured by many companies. Apart from mobiles they are also manufacturing smart tablets, and smart phones besides making much other hand held devices. The mobile services have become very popular. This has resulted in lacks of applications available for mobile devices like iPhone and Android [1]. Recently, with the invent of cloud computing, the mobile devices are able to participate in cloud computing as well. This is because; the cloud provides many benefits to mobile devices to have more flexibility and very rich set of communications. Advanced techniques and applications are possible now in mobile devices. They include multi-media content sharing, push notifications, phonebook, and so on. The mobile devices are actually resource constrained. However, when they re connected cloud, they become resource rich and they can participate in massive computational processing as the mobile cloud infrastructure enables this. The mobile devices can obtain services of cloud so as to enhance the quality of service being rendered to clients. There is practical convergence of cloud services and mobile computing that resulted in new devices. Virtualization is the technology that enabled realization of cloud computing in the real world. Virtual smart phone devices came into existence. For instance these devices came over IP [2] with the feature that enables creating virtual mobile instances. Each virtual device is can be used by an end user in order to perform operations. The virtual instances are having no resource restrictions. In fact, they have accessibilityto cloud infrastructurewhich represents multiple users, devices which are connected in the network.

In this paper, we focused on built architectureformobile infrastructure that enables mobile instances to participate in hug computations and storage. Since the devices are connected cloud, they can realize unlimited resources. However, the mobile cloud infrastructure can become vulnerable to attacks it if it does not have security in place. The serviceproviders should be able to have an idea about security issues involved and address them. As per IDC [3], many services providers opin3ed that it is important to implement security in mobile cloud computing. Recently many incidents came into surface that suggest the cloud infrastructure is vulnerable if specific security measures are not implemented [4], [5]. Malicious mobile application is another problem for mobile cloud services. When the applications are compromised they behave differently and they cause problems to the cloud besides

disrupting cloud services to end users. The main technologies used to make it possible are cloud computing which is on top of virtualization. Then we focus on abnormal behavior detection in mobile cloud infrastructure. Towards this the application monitors the mobile instances and their operations in order to secure the network. Abnormal behavior detection is the key issue resolved in this paper. Signature – based applications can run on virtual mobile devices to detect abnormality of nodes by studying infrastructure. However, it has overhead and difficult to end users to perform operations. To overcome this problem behavior based abnormal detection method is implemented in this paper. We built a monitoring architecture that takes care of security of the cloud applications in mobile cloud infrastructure. The remainder of the paper is structured as follows. Section II reviews literature on mobile infrastructure cloud. Section III provides details of the proposed work. Section IV presents experimental results while section V concludes the paper.

II. RELATED WORK

Since mobile devices cloud participates in the cloud to leverage the benefits of it, there were many researchers focused on the cloud computing with mobile devices. They focused on the security issues involved in the cloud infrastructure as well. For instance Shabtai et al. [6] built a framework that can detect malwarein Android mobile devices. They worked out on the features such as network usage, memory, CPU and other feature sin order to detect malware. For this purpose they used many algorithms that cloud monitor malware presence in mobile cloud applications and infrastructure. Later on in [7] also malware detection and spamming were explored. However, it was not a general purpose malware detection mechanism. They determined the behavior of mobile devices with respect to phone calls, SMS, and web browsing. They made use of machine learning algorithms that are powered by famous data mining tool named Weak [8]. The malware detection programs could work with highest accuracy. Many studies were focusing on the abnormal behavior of mobile devices when they participate in cloud computing. The studies defined the behavior of mobile devices so s to use them for further research. In [9], the authors related the privacy information on mobile devices and the abnormal behavior is detected. The framework could monitor the privacy data and monitor mobile devices that can detect abnormal behavior. Then Burguera et al. [10] correlated this behavior with the call counter, and then focused further on system calls for fining malware which generally accesses commands like chown(), chmod() and access. However, this framework has certain limitation as it needs root permission with respect to Android and other devices.

For monitoring abnormal behaviors in cloud infrastructure, many researches came into existence. The main focus is on the intrusion detection systems. In [11] Roskchke et al. discussed the architecture of IDS that can detect programs with malicious behavior. IDS monitor incoming and outgoing traffic and detect intrusions. Many management issues were aroused with respect to IDS. IDS have been enhanced to provide more security. They enhanced IDS are known as Host IDS (HIDS) and Network IDSS. The difference in them does not provide information about how malicious programs are treated by the IDS. Vieira et al. [12] proposed an IDS for cloud computing and also bgrid. They performed behavior analysis with respect to each one in the mobilecloud infrastructure. Their architecture lacksreal virtualization of nodes with virtual instances provided to end users as part of the infrastructure cloud. The analysis of the performance of the nodes is made in order to detect malicious behavior. This has helps in monitoring and detecting abnormality in mobile cloud infrastructure.

III. MOBILE CLOUD INFRASTRUCTURE FOR ABNORMAL BEHAVIOR

The aim of the mobile cloud infrastructure is to detect abnormal behavior in the cloud infrastructure that contains mobile devices, virtual mobile device instances. The cloud infrastructure has virtual mobile devices that can accommodate services to real mobile users. The connectivity is made through WiFi networking. The architecture for monitoring abnormal detection in mobile cloud infrastructure is as given in figure 1.

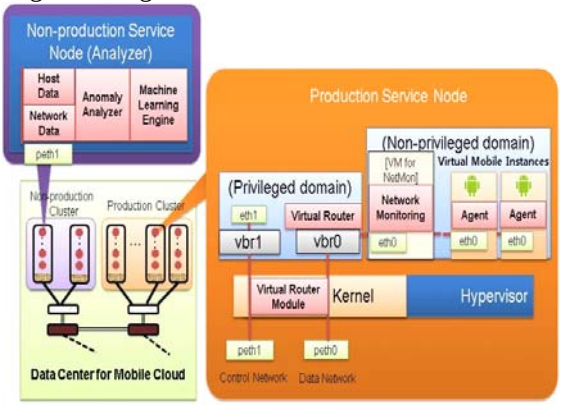

Fig. 1 –Architecture for abnormal behavior detection

(Excerpt from [13])

As can be seen in figure 1, the architecture has data center for mobile cloud, and production service nodes and non production service nodes. The data center for mobile could haveproduction and non production clusters. The non production service node acts as an analyzer which has host data, network data, anomaly analyzer and machine learning engine. The production service node has privileged domain and non privileged domain. The privileged domain takes care of routing while the non privileged domain takes care of network monitoring. The Hypervisor is used for virtualization to have virtual mobile instances.

Abnormal Behavior Detection

The analyzer presented in figure 1 makes use of machine learning algorithmsavailable in Weka [8] for abnormal behavior detection. Out of the algorithms available in Weka, in this paper, we used Random Forest (RF) algorithm to train data for abnormal behavior. This algorithm is the combination of decision trees that depend on the sampled random vector [14]. The collected features are represented as a vector with the train data that has been obtained from collected data. Three states of behavior have been defined by us. They are known as active, inactive and abnormal. Inactive doe meant that an instance is not being used for applications in the mobile cloud. From this state, it moves to active state when user starts using any application through that mobile instance. Abnormal state is the state in which a node is affected with malware or such malicious programs. More than 250 virtual hosts are created and tested. The results are presented in the following section. More information about the techniques and approach can be found in [13].

IV. EXPERIMENTAL RESULTS

We built a custom simulator to demonstrate the proof of concept. Java platform and Java mobile platform is used to simulate the mobile cloud infrastructure. The environment used to build the application is a Laptop with 4GB RAM running Windows 7 operating system. Experiments are made with nodes and their behavior. The nodes are in three states namely active, inactive and abnormal. The RF machine learningalgorithm is used to detect abnormal behavior. The results are as presented below.

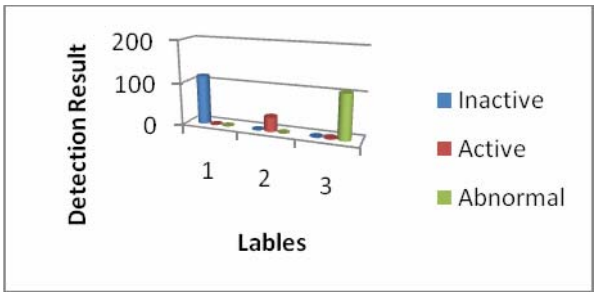

Fig. 2 – Experimental Results

As per the results the states are changing from inactive to active and then abnormal if the node misbehaves. The abnormal behavior is detected and presented in the results. False positive rate is negligible. It reflects that the proposed architecture is effective in abnormality detection in mobile cloud infrastructure. The RF machine learning algorithm has given accurate results. Figure 3 shows the results further.

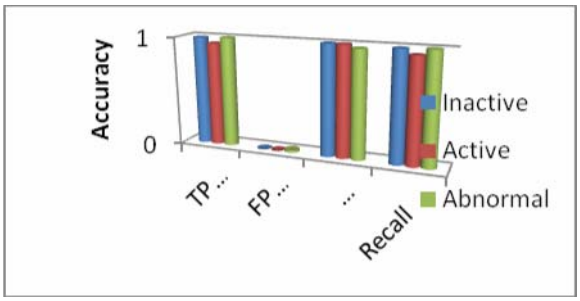

Fig. 3 – Accuracy of the detection

As seen in figure 3, the accuracy of the results is presented. For active, inactive and abnormal states the algorithm recognized accurately. It is evident in the true and false positives besides precisions and recall measure. The weighted average also shows the negligible false positives. This will prove that the proposedmethodology is effective and can be used in the real time applications.

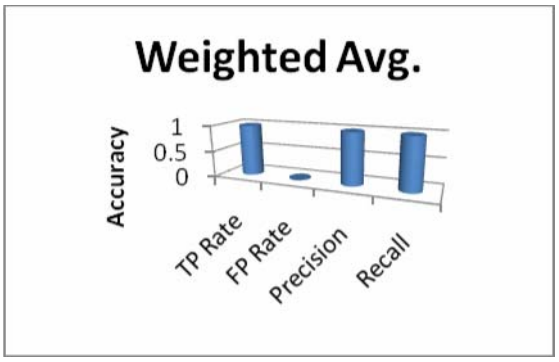

Fig. 4 – Weighted Average of Evaluation Methods

As can be seen in figure 4, the evaluation process has involved finding true positives, false positives besides precision and recall. The results reveal that the architecture proposed has shown negligible false positives rate. This shows the effectiveness of the approach.

V. CONCLUSION

In this paper we studied the security issues in mobile cloud infrastructure. Our main focus is on monitoring and detecting abnormal behavior in mobile cloud infrastructure. Many scenarios of usage of the proposedinfrastructurearediscussed. The virtual mobile instances were created as part of the mobile cloud infrastructure. We have implemented the methodology proposed by Kim et al. [13] for addressing secure issuesin the infrastructure. We also built an application which simulates the proof of concept. The empirical results that the mobile cloud infrastructure built on the given architecture is affecting in providing security to the communications in the mobile cloud.

REFERENCES

[1] Distimo, "The battle for the most content and the emerging tablet market", April, 2011, http://www.distimo.com/blog/2011_04_the-battlefor- the-most-content-and-the-emerging-tablet-market/.
[2] E. Y. Chen and M. Itoh, "Virtual Smartphone over IP", The next IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM 2010), Montrreal, Canada, June 2010, pp.1-6.
[3] F. Gens, "IT Cloud Services User Survey, pt.2: Top Benefits & Challenges", IDC eXchange(http://blogs.idc.com/ie/), August 14, 2008.
[5] 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.
[4] 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.
[6] 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.
[7] 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.
[15] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and H. Ian, "The WEKA Data Mining Software: An Update", SIGKDD Explorations Newsletter, Vol. 11, No. 1. New York, NY, USA, June, 2009, pp. 10-18.
[8] 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.
[9] 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.
[10 S. Roschke; F. Cheng; C. Meinel, "Intrusion Detection in the Cloud", Dependable, Autonomic and Secure Computing, 2009. DASC '09. Eighth IEEE International Conference on, Chengdu, China, December 12-14, 2009, pp.729-734.
[11Vieira. K, Schulter. A, Westphall. C.B, and Westphall. C.M, "Intrusion Detection for Grid and Cloud Computing", IT Professional , vol.12, no.4, July-Aug. 2010, pp.38-43.
[12Taehyun Kim, Yeongrak Choi, Seunghee Han, Jae Yoon Chung, Jonghwan Hyun, Jian Li, and James Won-Ki Hong, "Monitoring and Detecting Abnormal Behavior in Mobile Cloud Infrastructure". IEEE, 2012.
[13 L. Breiman, "Random Forests", Machine Learinig, Vol. 45, No. 1, 2011, pp.5-32, DOI: 10.1023/A:1010933404324.

AUTHORS

1.Supraja.Y, is pursuing M.Tech (CSE) in QIS College of Engineering and Technology, Ongole, AP, INDIA. She has Completed M.C.A degree.Her Research area datamining and network.

2.TV. Sai Krishna completed his M.Tech from JNTU Anantapur in 2007.He completed his B.Tech in CSE from JNTU HYDERABAD in 2004. He is currently pursuing his Ph.D from JNTU Kakinada. Research interests include Image processing ,Data Mining and Computer Networks. He published many papers in several Journals and Conferences. He is a Member in various professional bodies like ISTE, CSI, IE.

3.Venkata SubbaReddy P has 11 years of teaching experience. He has published more than 20 papers in various International journals. He is member of various International & national journals. He is a life member for ISTE .

4. Dr.M.A.D.Swamy is currently working as professor in CSE Department. He has 18 years of the teaching experience. Published various papers in journals and attended conferences and member for journals. Member in ISTE.

5. Dr.P.Srinivasulu is currently working as professor and H.O.D in CSE Department. He received Ph.D .in Acharya nagarjuna university guntur in 2011 and published various papers in journals and conferences.