IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Monitoring the Security Issues in Service Delivery Models of Mobile Cloud Infrastructure

MaheshwariBhavani.D[1], Apirajitha.P.S[2]

[1, 2]**Department of Sree Sastha Institute of Engineering and Technology, Chennai, Tamil Nadu, India**

Abstract

At recent trends several mobile services are changing to cloud based mobile services in which a mobile cloud infrastructure is deployed which combines mobile devices and cloud services to provide virtual mobile instances through cloud computing . In this project cloud services are virtualized to the mobile through the mobile cloud infrastructure. It is the combination of the mobile and the cloud service it leads to many security threats and faults while delivering the service and it is detected through certain anomaly detection algorithms and fault detection frame works . In this paper malicious agents enters into the cloud infrastructure and it is detected in the cloud by not allowing the anomalies to be entering into the mobile.

Keywords: Mobile cloud infrastructure, virtual mobile instances, fault detection, anomaly detection.

I. Introduction

Cloud computing refers to the infrastructure in which application are delivered as the service over the internet .These infrastructure are supported by very large networked distributed machines (distributed machines are the one. Here is an emerging concept called cloud- based mobile services benefits users by richer communications and higher flexibility. Massive computational processing is performed through cloud computing Infrastructure The data stored in the cloud infrastructure can be accessed at any time and from anywhere through mobile devices i.e it provides the virtual instances from the cloud to the mobile. In this paper we present a mobile cloud infrastructure that provides virtual mobile instances and those instances are managed in the cloud computing architecture. The instances may be resource access or storage capability.

According to the IDC report the main problem in the cloud computing is the security.IDC refers to the international Data Corporation is an American research firm specilizing in Information Technology.

In this it provides event monitoring a web based visualization interface for allowing the system To validate this methodology, a mobile cloud infrastructure is built and then intentionally malicious agents are injected in to the cloud and this is monitored and detected in the cloud through the fault detection framework which includes a cloud administrator and also using an automated fault detection algorithm. This framework will acquire more efficiency and accuracy than the existing frame work . This monitoring architecture will not allow the anomalies to enter in to the mobile from the cloud. Another concept called virtualization is deployed in this paper.Virtualization is an outstanding technology which allows rich control of physical resources, enabling full exploitation of the machine's capacity at a negligible overhead cost. This offers high degree of control over the sharing of the physical resources. In this way the resources are accessed from the cloud to the other resources.

II.Existing Work

In the existing work many frame works had been built for the security and the accessing of the resources in the mobile cloud. In the existing work, a scheme called virtual smart phone over IP [3] had been deployed. In this it allows the users to create virtual smart phone images in the mobile cloud and to customize each image to meet different needs. Users can easily and freely tap in to the power of the data centers by installing the desired mobile applications remotely in any one of these images. But in this scheme the security is vulnerable where the images also contains some malware data or untrusted applications and the detecting scheme for this data is not that much effective.

In the existing system the anomaly detection is mainly based upon the behavior of the system, based upon the behavior the intrusions are detected[7] . In this process the data sets are collected from the smart phone users and their behavior are analyzed and the

intruder is found based upon the previously collected behavior it is completely behavior based and not signature based, the major disadvantage of this is that it is applicable only for the iphones.

The next approach for the smart phone is the tain troid [8], an flow tracking device is used for tracking the sensitive data of the smart phone , where the smart phones are monitored for its misbehavior while handling the private data. But this is applicable only to a few smart phone devices .It can track only a few smart phone devices and it is not applicable for the monitoring of the huge smart phones.

Another approach in the existing is that monitoring and detecting the abnormal behavior in the mobile cloud infrastructure [1] ,In this the malware data in the mobile cloud infrastructure is detected through the machine learning algorithm called the random forest algorithm where these algorithm works based upon the datasets collected through the analysis process and these training datasets are used to draw a decision tree and that decision tree is pruned ,from the pruned decision tree the decision is made whether the data contains malware are not . In this procedure then it is not accurate and based upon the behavior only the decisions are made and it is the time consuming process.

All the approaches in the existing does not reveal the user security while accessing the cloud as these are done in the public cloud, they only reveals about the smart phone security. This is another major drawback in the existing system. If suppose a user access the cloud and there will be a chance for the Intruder to access the cloud without any authorization These type of security is not provided in the previous existing approaches. They only talk about the smart phone security and how to detect the malware etc . These are the major disadvantage in the existing system.

To overcome the above existing disadvantages a proposed frame work of monitoring the security issues in service delivery models of the mobile cloud infrastructure is proposed.

III.Proposed System

In the proposed system monitoring the security issue in the service delivery models of the mobile cloud infrastructure is proposed . In this proposed system the cloud services are virtualized to the mobile through the mobile cloud infrastructure. It is the combination of the mobile and the cloud service it leads to many security threats and faults while delivering the service and it is detected through certain anomaly detection algorithms and fault detection frame works. In this paper malicious agents enters into the cloud infrastructure and it is detected in the cloud by not allowing the anomalies to be entering into the mobile.

In addition to this it also provides the user security in the public cloud by Base-64 encoding algorithm , where the user access to the cloud such as the username, password are encoded using the Base-64 algorithm and the faults or the anomalies are found using the Fault detection framework.

In the fault detection frame work, a mobile cloud infrastructure is built and then intentionally malicious agents are injected in to the cloud and this is monitored and detected in the cloud through the fault detection framework which includes a cloud administrator and also using an automated fault detection algorithm. This framework will acquire more efficiency and accuracy than the existing frame work . This monitoring architecture will not allow the anomalies to enter in to the mobile from the cloud.

IV. Related Work

A. Cloud Service and Scenarios

This section defines a mobile cloud service through the virtualization of mobile devices in cloud infrastructure. This cloud infrastructure or the architecture is first built in the desktop using the cloud operating system called the eye operating system. This provides the cloud platform inside the desktop, where any type of files can be uploaded and applications can be maintained in this cloud architecture and certain services from the cloud is discussed.

B.Concept of Mobile Cloud Service

In this work the virtualization of the mobile devices in the cloud infrastructure is done , where it is done by registering the smart phone specifications in the cloud and the user is given the authorization to access the cloud and access the resources virtually from the cloud. This mobile cloud services provides virtual mobile instances through the combination of a mobile environment and the cloud computing. Virtual mobile instances are available on mobile devices by accessing the mobile cloud infrastructure. This means that the users connect to virtual mobile instances with their mobile devices and then use the computing resources on the mobile cloud infrastructure.

C.Cloud Administrator and Proxy Process

In this process a cloud administrator is provided and the admin has all the rights to give access to the user or to upload a file etc. The admin will provide the encoded password to the users who are accessing the cloud via the smart phone . The files which are uploaded in the mobile cloud are also saved in the encoded format using the Base-64 algorithm.

A proxy server is the one which is the proxy for the cloud server where it contains all the details about smart phones and its user. It will maintains the details such as the how many users are registered and which user uses which type of the smart phone etc ,these type of information are stored in the proxy server. It also forward the request from the smart phone to the cloud server.

D.Monitoring Abnormal Behaviour in Cloud Computing Infrastructure

In this frame work the main task is finding the misbehavior in the cloud while browsing any files from the smart phone. If suppose a user browses a text file and if contains any anomaly it is detected in the cloud using the automated fault detection algorithm. In this frame work malicious agents are injected in to the cloud test bed and these are detected using the algorithm.

The architecture for the mobile cloud infrastructure and the overall structure to detect abnormal behavior in the infrastructure illustrates that mobile nodes are divided into production service and non-production service nodes. Production service nodes are a group of service nodes providing services to customers directly, and non production services are the one which supports mobile cloud services indirectly, such as through the processing of back ground jobs. It also the monitors the host and the network data.

These data can be monitored using the agent programs which are installed in each virtual mobile instance. It can monitor mobile host information in detail, including the CPU and memory usage in virtual mobile instances. This fault detection framework detects the malware data and it will not allow the malware data to be enter into the mobile and it will give prior information that anomaly is detected to the smart phone as a warning or an alert. By this way the infected files can be preventing from entering into the smart phones this is detected inside the cloud environment itself. The proposed architecture is shown in the figure .1.

V.Proposed Architecture

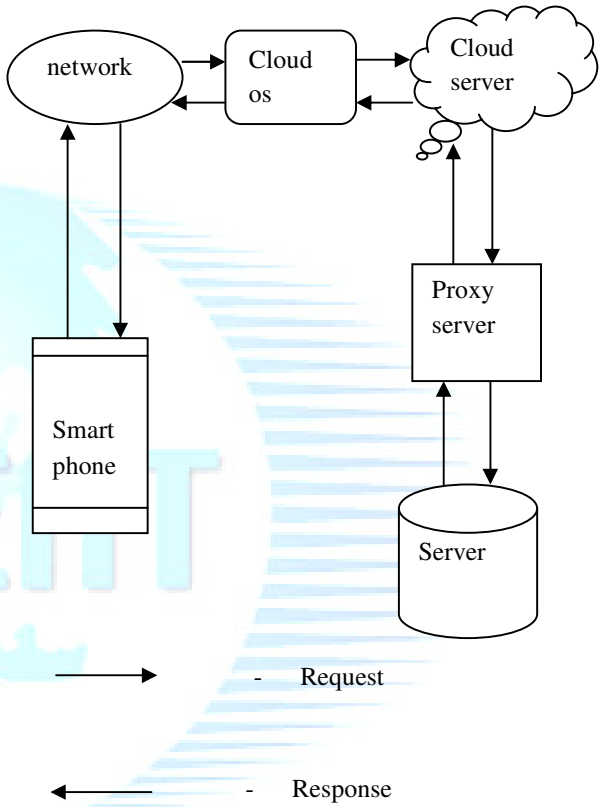

Fig . 1. Proposed architecture for the detecting the anomaly

The fig .1 shows the proposed methodology . In this first the request for the files is sent from the smart phone to the cloud. This request is taken to the cloud server where it is passed to the main server via the proxy server, the proxy server forwards the communication from the smart phone to the server. The server gives the requested file and it taken to the smart via the cloud server, In the cloud the cloud administrator will check whether the upcoming request and the response is coming from the authorized user or not. Then the automated fault detection algorithm in the cloud will finds the information about the data whether the data contains any malware, If it contains any malware means, the information is immediately sent to the smart phone as a warning or alert. This is the work behind the architecture.

VI.Algorithms Used

A. BASE- 64 ENCODING ALGORITHM

The user security is provided to the smart phone users as this project is deployed on the public cloud there is a chance for the intruder to break the system or it will lead to the unauthorized use of the system in order to overcome this security threat, the login details and the communication between the cloud and the user is encoded with the Base-64 encoding algorithm . The files that are uploaded in the cloud also has been encoded using this Algorithm.

ALGORITHM DESCRIPTION:

- Base 64 is an encoding scheme which is designed to allow binary data to be represented as ASCII text.
- Base64 encoding schemes are commonly used when there is a need to encode binary data that needs to be stored and transferred over media that is designed to deal with textual data. This is to ensure that the data remains intact without modification during transport. Base64 is commonly used in a number of applications including email , and storing complex data .

B.FAULT DETECTION FRAMEWORK IN CLOUD

An automated fault detection framework for cloud system FDCS which runs on top of the admin's system. The algorithm is entirely decentralized; as a result does not burden any single machine with excessive workload and at the same time does not require all the data to be centralized for execution. FDCS takes all the measurements of network systems into consideration and reports a ranked list of the machines based on its anomaly or fault score. Moreover, for each machine in this list, a system administrator can display the faultiest variable which caused the anomaly. The algorithm uses distance based anomaly definition to identify if a machine is faulty or not. It is extremely fast and can run continuously on changing data, thereby allowing an uninterrupted monitoring of the machine performance. Using FDCS, one can take corrective actions early before they become fatal faults and thereby degrading the overall system performance.

It is done using the below mentioned algorithm where the admin system maintains all the record of the client machines and this algorithm runs on the admin system and the admin system monitors all the data and the communication in the client machines that is described in the below algorithm were it explains that it will check all the blocks of the data Di and this will go for the blocks of the data, the checking is done block by block ,then its nearest neighbor values are classified and the analysis is performed by comparing all the system, if any changes is noticed or if any misbehavior is detected means it is immediately forwarded to the smart phone and these detection process will run on the cloud environment itself.

This fault detection framework will gain more accuracy in finding the anomalies this is not only behavior based but also it is knowledge based ,It allows the sytem to analyse its performance and the general behavior based upon this behavior the analysis is performed.

In the existing the algorithm called the random forest algorithm is used to detect the anomaly this algorithm is knowledge based based upon collected dataset priorly its decisionmaking time is high when compared with the proposed algorithm.

ALGORITHM: Fault Detection Algorithm

Procedure PUSH_ Anom()
begin
for all blocks of data in Di do
B ← getNextBlock (Di);
for all points b ∈ B do
Lk(b) ← ∅;
for all points x ∈ Di do
for b ∈ B, b 6 = x do
if dist(b, x) < rb or |Lk(b)| < k then
Update Lk(b) with x by removing
the farthest point;
remove b from B;
τi ← τi+ 1;
for b ∈ B do
Send (b, Lk(b), rb) to machine Pi+1
mod p;
Call PULL Anom();

The above algorithm is the automated fault detection algorithm for the cloud where it is an automatic process in which these detection process is taking place inside the cloud itself. It checks each and every activity of the client machines and checks for the report with the nearest machines. Fault Detection in Cloud Systems (FDCS) framework in which the participating machines in a cloud computing

environment can collaboratively track the performance of other machines in the system and raise an alarm in case of faults.

VII.Comparison Analysis

In the existing work only it is said about the cloud security and not said about the secure storage and user security. The algorithm used in the existing system is random forest algorithm for the anomaly detection in the cloud, this algorithm is a behavior based using the prior knowledge and will not provide automated response at the security threatening environment and the decision making time of this algorithm is high, but proposed fault detection algorithm detects the anomalies by continuously analyzing each participating machines in a cloud computing environment can colloboratively track the performance of other machines in the system and raise alarm in case of faults, this automated response is not provided in the existing and the Base-64 encoding format is not provided in the existing system which provides additional security to the cloud. The percentage of security in the mobile cloud Infrastructure in the proposed will be expected to be high than the existing.

VIII. Conclusion

In this paper, a new mobile cloud service with the virtualization of mobile devices is deployed and discussed some possible security issues. To address security issues in mobile cloud infrastructure, fault detection methodology using automated fault detection algorithm and architecture to detect malware is proposed. This proposed methodology will gain more accuracy than the existing system is concluded from the analysis performed. Further, the other monitoring features to improve the accuracy of detecting the faults are considered and also the performance metrics are also have been considered.

REFERENCES

[1] Taehyunkim , Yeongrak choi , Seunghee Han "Monitoring and detecting abnormal behavior in the mobile cloud infrastructure" 2012 IEEE/IFIP 3rd Workshop on Cloud Management.

[2] 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.

[3] 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.

[4] F. Gens, "IT Cloud Services User Survey, pt.2: Top Benefits & Challenges", IDC exchange (http://blogs.idc.com/ie/), August 14, 2008.

[5] 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] 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] 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 : behavior based malware detection system for android", Proceedings of the 1stworkshop on Security and privacy in smart phones and mobile devices (SPSM'11), New York, NY, USA, October 17, 2011.

[10] 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.

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

[12] L. Breiman, "Random Forests", Machine Learinig, Vol. 45, No. 1, 2011, pp.5-32, DOI: 10.1023/A:1010933404324.