Malware Propagation Detection in Mobile Cloud Infrastructure with Architectural Change

[1]Vengali Sagar, [2]V. Ravi Kumar,
[1]*PG Scholar, Department of Information Technology, TKR College of Engineering and Technology Hyderabad, A.P-500 097, India*
[2]*Assistant Professor, Department of Information Technology, TKR College of Engineering and Technology Hyderabad, A.P-500 097, India*

Abstract: —
Now a day's a lot mobile services are converting to cloud depended mobile services with highly communications and higher flexibility. We explore a unique mobile cloud infrastructure that attaches mobiles and cloud services. This fresh infrastructure gives mobile instances which are virtual among cloud computing. To enter into marketing level various services containing this type of infrastructure, the people which give providers service have to know about these security openings. In this paper, we initially declare different mobile cloud services get into mobile cloud infrastructure and to discuss the security threats that might be chance through the usage of many service scenarios. Then, we explore architecture and methodology for abnormal behavior detection through the observation of host and network data. To check our methodology, we inserted malicious programs into our mobile cloud test be and utilized a machine learning algorithm to find out from those programs the abnormal behavior that arise.
Keywords: Mobile cloud computing, mobile cloud infrastructure, mobile cloud service scenarios, abnormal behavior monitoring, machine learning.

I. INTRODUCTION

In order with the diverse electronics manufacturers gives new mobile devices like smart tablets and smart phones, different mobile services are being given as devices applications. There are more than two millennium Android and three millennium iPhone apps given [1] as of March 2011 and these numbers have growth. Latest recent trend for mobile services are there to vary to mobile services of cloud. Mobile services of cloud satisfy users by communications which are rich and max flexibility [1][2][3]. Rich communications refers techniques which are advanced supports features like such as enhanced messaging, phonebooks with, enriched call and push notification additional with multi-media content sharing. Max computational processing is operated through cloud computing infrastructure rather than of low-speed mobile devices [3]. The information which was placed in cloud infrastructure can be used whenever we need through mobile devices. Finally as outcome, high level communications and flexibility which was higher can be given to mobile device customers through cloud computing only. Via mobile devices convergence and services of cloud, we estimate that new mobile cloud services will be offered with the mobile devices virtualization in cloud infrastructure. Over IP Virtual Smartphone is one example of virtual [6] [8] mobile provisioning instances to users. In cloud infrastructure every virtual instance represents a mobile device, and Users can use this instance by connecting to it. In this paper, we explore a mobile cloud infrastructure that offers virtual mobile instances, and instances which are maintained in architecture of cloud computing with huge computational processing storage and power. Although apps which were signature-based vaccine can focuses on virtual mobile instances to find out malware, it creates additional overhead on instances, and it is tough for customers to use vaccine software by pressure when such instances are given like service. Behavior-based abnormal detection capable of detecting that crisis by keeping eye on operations in the cloud architecture. To gain this, we implement a monitoring architecture utilized for both the network and host data. With the help of monitored data, abnormal behavior is founded by using a algorithm of machine learning. To check our methodology, we constructs a test floor for infrastructure of mobile cloud, malicious mobile programs which were installed intentionally onto different virtual mobile instances, and then efficiently detected the abnormal behavior from those malware programs will get emerged.

II SYSTEM MODULES

Mobile Cloud Service: Explaining "mobile cloud computing" is premium one for explanation and characterization of cloud services in mobile. There are a lot descriptions of cloud computing in mobile that allocate big role to devices of mobile for cloud computing. Some researchers described mobile [13][17]

cloud computing as using the cloud via mobile devices at the same time mobile have been part of huge cloud architecture. Some of them referred to as a term of mobile cloud computing meaning that a lot of mobiles implement a cloud computing group, and jobs are placed to different device nodes in a way to implement faster computing jobs.

Service Scenarios for Mobile Cloud Services

Variant users:

Individual users are categorized as advanced users, normal users and developers based upon age types and their requirements [1].

1. Normal Users: These users are keeps concern in the services which are available from the mobile cloud environment. The cloud environment needs by these users is somewhat fixed with little change is must.
2. Advanced Users: These users are well known of mobile cloud services overview and keep more concern than normal users in cloud resources. They need a cloud environment that changes more frequently.
3. Developers: These users are having good knowledge overall mobile cloud services and need a cloud environment which was specified, differs and which moulds frequently.

Normal User			
Place	Device	Network	Consuming Content
Travel	Tablet	3G/4G	Online game, movie
Home	Laptop	Home Wi-Fi	Movie
Advanced User			
Place	Device	Network	Consuming Content
Office	Smart phone	Office Wi-Fi	Smart work
Bus	Laptop	3G/4G	Simulation
Developer			
Place	Device	Network	Consuming Content
Travel	Tablet	Public Wi-Fi	Server management
Home	Tablet	3G/4G	Readbigsize data

TABLE I. INDIVIDUAL USERS USAGE[1]

We show one service scenario sample for users which are individual. This is a mobile app scenario for developers who implement mobile apps and run a server for the application in cloud.

• Actor: Mobile app Developers

• Concerns:

 To implement and test mobile app in various mobile environments.

• Conditions:

 Mobile cloud service have to various mobile environments customizing function.

 User requires a lot mobile environments with various hardware resources and display size.

 User accesses every virtual mobile instance and checks application whether or not it operates well in various environments through Wi- Fi public with tablets.

 User/Actor needs virtual mobile instances additionally with efficient hardware resources and utilizes it as a server for application.[2]

Office workers

We made office workers into different categories as main office staff, overseas offices staff and subcontractors related to their location of office and relationship to the company [8][9]. Assigning that a mobile office system is installed in the main office; Table II provides a summary of possible service scenarios with various requirements for every case of office workers. Main office Staff: These users operate on mobile office systems which were installed in the main office.

1. Overseas offices Staff: From overseas offices these users operate mobile office systems to the main office. Abroad there may be poor network condition than domestically mobile offices accessing. Therefore these actors have concern in a stable mobile office environment.
2. Subcontractors: These users contract as main office developers, co-work or run a project with the respect company. If their commitment is no longer valid, subcontractors should not utilize mobile office systems given from the main office.

Staff in a main office			
Place	Device	Network	Consuming Content
Travel	Smart phone	3G/4G	Messenger, Schedule email
Office	Laptop	Office Wi-Fi	Word, VoIP
Home	Tablet	Home Wi-Fi	Word, Approval
Staff in overseas Offices			
Place	Device	Network	Consuming Content
Customer office	Smart phone	Public Wi-Fi	Document view
Office	Laptop	Office Wi-Fi	Payment, video conference
Sub contractors			

Place	Device	Network	Consuming Content
Office	Laptop	Office Wi-Fi	Program development
Outdoor	Smart phone	Public Wi-Fi	Project management

TABLE 2. OFFICE WORKERS Usage[1]

The example of service scenarios for workers of office: overseas offices staff.

• Actor: Overseas office staff

• Concern:

 To use mobile office environment in mobile cloud with max speed and overseas stability.

• Primary conditions:

 Special network channel such as VPN should be set to guarantee high speed connection between overseas office and mobile cloud infrastructure.

• Main Theme

 Actor uses mobile office and shares multimedia files to co-workers in the main office with max speed connection.

 Actor uses mobile office through public Wi-Fi and test the payment. Still network connection is not stable because of poor network environment; he can continue his work by accessing mobile office again.

Network and Host Features

The analyzer utilizes gathered data from third parties in virtual routers, and virtual mobile instances to find abnormal behavior.

➢ Host Features

In each virtual mobile instance if we take the root permission, then we can see each event, additional with kernel-level information, and we can find abnormal behavior more accurately and efficiently. Although, rooting describes that it is simply exposed to abnormal behavior and form more typical than normally be the issue. Thus, in this paper, our third parties mobile application won't need permission to root; rather it collects the data with user permission which was general, not permission to root. Researchers analyzed the relation among malware behavior and possible monitoring features. Although, the monitoring features count is more than half century with lot of them giving low dependency. So, we select about couple of decade features among the half century which explore max dependency on abnormal and normal behavior, and which are described in Table III. Network features [5]

➢ Network Features

Three Malware types are presented of that use network resources.

• In virtual mobile type 1 hacks data instances which was invisible to the user and forward them to an external server.

• And another one spoils virtual mobile instances as zombie and utilizes them to construct botnet and DDoS attack.

• Last one maximizes usage of network so that over-charged will be done for communication fare.

Network Features
Number of Hosts
Number of Packets
Number of Flows
Size (Bytes)
Number of DNS Packets
Number of HTTP Packets
Number of HTTPS Packets
Number of Well-known port Packets
Number of Other port Packets

Table: .Monitoring Features At The Network Level

III RELATED WORK

Previous methods concern about the detection of malware by observing the nature in mobile. Developers discovered a framework of behavioral to find out malware operations for the sake of mobile devices which are of Android. They extended the qualities of memory, CPU and uses of network, observed these

utilizing their mobile apps, and next caught malware using lot algorithms of machine learning. Developers targeted on malware that are similar to spamming, even though method won't get detect high amount of normal malware [4][5]. They declared the mobile devices behavior as web browsing, phone calls, SMS, and were capable to find abnormal behavior utilizing machine learning algorithms that are presented in Weka with max accuracy. There are some more researches that also concern on mobile devices abnormal behavior, but those researches declared the behavior of mobile devices different. Abnormal behavior of mobile devices to privacy data on mobile devices.

Abnormal Behavior Detection

The analyzer works on algorithms which are machine learning with the help of Weka tool. Machine learning algorithm Random Forest (RF) was used to coach abnormal behavior with our gathered data set. The RF algorithm is a set of decision trees that every tree based on the random vector values a sampled which was independent and with the distribution which was same for all forest trees. We explored the gathered features as a vector subsequently with the data used to coach our gathered data set. We described three behavior states: abnormal, active, and inactive[6]. An inactive state is nothing but that the instance is not utilized and some apps are working in the background. If the user utilizes the instance and operates games, web browser, or other apps, then the host transforms into an active state. If single or more working/running apps are founded as malware by continuously needing delivering local or root privilege information to particular remote servers, then the host is allowed to be in an abnormal state. From the virtual mobile host we collected completely 257 sample information; for 116 minutes inactive data, for 36 minutes active data, for 105 minutes and abnormal data.

CPU (%)	Memory (KB)	Process
CPU Usage (User)	Free Memory	CPU Usage
CPU Usage (System)	Active Memory	# of Thread
	Inactive Memory	Memory Usage
	Anonymous Memory	Context Switches
	Mapped Pages	Non-voluntarily Context Switches
Network	**OS**	Total Tx Bytes
3G Tx Packets	Running Processes	Total Rx Bytes
3G Tx Bytes	Context Switches	
3G Rx Packets	Process Created	
3G Rx Bytes	Process Blocked	
Wi-Fi Tx Packets		
Wi-Fi Tx Bytes		
Wi-Fi Rx Packets		
Wi-Fi Rx Bytes		

Table Iii.Monitoring Features Using Agents

IV CONCLUSION

With the help of RF machine learning algorithm detecting abnormal behavior explores that our proposed method is efficient one in the detection of abnormal behavior. For further process, research on feasibility service for mobile cloud service. We will also calculate the efficiency of our proposed monitoring architecture. To handle security issues on this service, we will collect different additional types of malware sample for practice in a way to increase the efficiency of using different machine learning algorithms. In future, we will take different monitoring qualities to increase the efficiency of abnormal behavior detection. But there is a crisis overhead like battery life and time complexity if we collect more features. So we have to undertake this issue together.

REFERENCES

[1] Monitoring and Detecting Abnormal Behavior in Mobile Cloud Infrastructure 1Taehyun Kim, 1Yeongrak Choi, Seunghee Han, 3Jae Yoon Chung, 3Jonghwan Hyun, 3Jian Li, and 1James Won-Ki Hong

[2] Scott Paquette, Paul T.Jaegar, Susan C.Wilson. Identifying the security risks associated with governmental use of cloud computing, Journal of Government Information Quarterly 27, pages 245-253, April, 2010.

[3] Arnon Rosenthal, Peter Mork, Maya Hao Li, Jean Stanford, David Koestar, Patti Reynolds. "Cloud Computing: A new business paradigm for biomedical information sharing". Journal of Biomedical Informatics 43, pages 342-353, August, 2008.

[4] Ann Cavoukian, Information and Privacy Commissioner of Ontario. "Privacy in the Clouds", A White Paper on Privacy and Digital Identity, 2009.

[5] R Gellman. “Cloud Computing and Privacy”. Presented at the World Privacy Forum, 2009.
[6] Subra Kumaraswamy, Shahed Latif and Tim Mather. “Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance”. Published by O’Reilly, 1st edition, September, 2009.
[7] Dan Svantesson, Roger Clarke. “Privacy and consumer risks in cloud computing”. Privacy consumer risks journal, pages 391-397, July, 2010.
[8] Kim Zetter. “Medical Records: Stored in the Cloud, Sold on the open Market”, Journal of privacy, crime and security, pages 223-256, March, 2009.
[9] Roger Clarke. “Evaluation of Google’s Statement against the rivacy Statement Template of 19 December 2005”, <http://www.rogerclarke.com/DV/PST-Google.html>, 2005.
[10] Google Docs Privacy Policy (Version of 3 October 2010). <http://www.google.com/intl/en/privacypolicy.html>, at 10 October 2010.
[11] Frank Gens. “IT Cloud Services User Survey, part 2: Top Benefits and Challenges”, Survey conducted by IDC, October, 2008.
[12] Buyya R, Yeo, Venugopal CS, S Broberg, J Brandic, I. “Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility”. Future Generation Computer Systems 25, pages 599-616, 2009.
[13] J.D Blower. “GIS in the cloud: Implementing a web map service on Google App Engine”, Proceedings of the 1st International Conference and Exhibition on Computing for Geospatial Research and Application, Washington D.C, June 21-23, 2010.
[14] Mark Nicolett, Jay Heiser. “Accessing the security risks of cloud computing”, Gartner Inc., June, 2008.
[15] Manish Pokharel and Jong Sou Park. “Cloud computing future solution for e-Governance”, Proceedings of 3rd International Conference on Theory and Practice of Electronic Governance, IEEE 2009.
[16] Ortuatay B. “Twitter service restored after hacker attack”, Journal of the Baltimore Sun, 2009.
[17] Cubrilovic, N. “Letting Data die a natural death”, International Journal of electronic Government Research, 2009.