DETECT AND IMMUNE MOBILE CLOUD INFRASTRUCTURE

A.Malathy[1], J.Gayathri[2], T.A.Vijayalakshmi[3], M.Ramkumar[4]

[1]PG Scholar, Department of computer science, Knowledge Institute of Technology, Salem, Tamil Nadu
[2]PG Scholar, Department of computer science, Knowledge Institute of Technology, Salem, Tamil Nadu
[3]PG Scholar, Department of computer science, Knowledge Institute of Technology, Salem, Tamil Nadu
[4]Department of computer science, Knowledge Institute of Technology, Salem, Tamil Nadu

Abstract

Mobile devices with cloud based service are highly effective and they are very flexible and adaptable. Mobile cloud infrastructure is a new concept where mobile devices and cloud services are clubbed together. As it a commodity, service providers should know the security issues. In this paper various security threats are widely discussed based on situation. A new methodology is proposed in order to detect the abnormal behavior. By detect the host and the communication channel certain malicious programs are injected in the test bed in order to identify the abnormal behavior. Using machine learning algorithm, these suspicious programs are detected. To find the next neighboring node and to detect the fault, FDMC algorithm is implemented.

***Keywords:** Fault Detection, Virtual Mobile Instances Signature based.*

---***---

1. INTRODUCTION

Different mobile services are provided as application to electronic gadgets like smart phones, tables and cloud based mobile services benefit users by providing enormous flexibility and wealthy communication. Data can be retrieved, processed and send at any time using mobile devices. Flexibility is there when mobile devices are accessed using cloud computing.

Each virtual instance is denoted by a mobile device and users can connect and make use of it.

Virtualization in mobile devices in cloud platform provides virtual instances to the mobile users. Virtual cloud infrastructure gives the virtual mobile instances. These instances are managed using extensive power and storage capacity. Virtual smartphone over IP is a classic example of virtual mobile instances. The threatening thing for the service provider is the security.

Even through signature based preventive algorithms are used in the virtual mobile instances, in order to find the malicious and suspicious applications, which basically run on the mobile cloud environment in the mobile cloud infrastructure certain malicious programs are injected which actually spreads the entire cloud and affects the commuting devices as well. Using FDMC algorithm to find the next neighboring node and detect the fault. Certain signature based vaccine are injected in the cloud in order to keep trace the malfunctions in the cloud instances.

By monitoring the data, suspicious behavior can be detected using the machine learning algorithm. In order to validate these methodologies a test bed is created which is basically a platform to test large projects. In this paper the entire concept is classified in to different section.

- Detecting the suspicious behavior in the cloud infrastructure.
- Security aspects and the possible situations of attacks
- Monitoring the architecture of the cloud infrastructure.
- Correct validation for the proposed architecture.
- Monitoring metrics needs to be configured for providing services and charging the users

1.1 Cloud Services based on Certain Situations

Based on the virtualization concept certain malicious mobile applications are allowed to execute in the virtual mobile instances and if any program attacks the cloud, it leads to major problem. This paper focuses on the abnormal behavior in the cloud infrastructure

Continuous monitoring is essential in order to find the malfunction in the cloud. So monitoring architecture is created to check both host and the data network flow. Using machine learning algorithm the unusual behavior is detected by implementing in the test bed environment.

1.2 Mobile Devices as a part of Cloud Construct

Mobile computing assigns different roles to mobile devices. Assigning the cloud through mobile devices is generally termed as mobile computing. Different mobile devices form a cloud group and various jobs are delegated to different mobile devices to perform the job faster in the cloud computing infrastructure.

Users may execute mobile application on demand services based on their needs. So the service providers also get benefited and obtain more profit. Perhaps this would have been better if the services are free of malware. So monitoring the entire host and entire data is a feasible host.

Machine learning techniques and monitoring real time traffic is a solution.

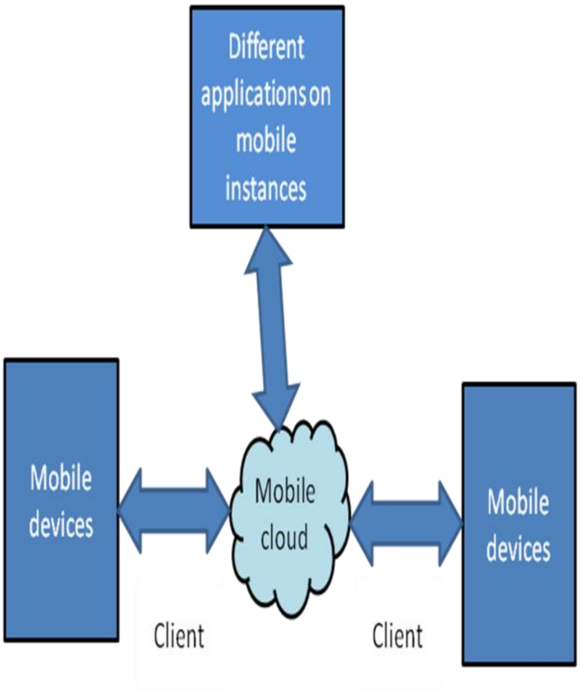

Fig 1: Mobile instances vs. mobile cloud

2. Detecting the Suspicious Behavior

Behavior determines what application runs on the mobile cloud infrastructure. Application creates flow between internal or external. These actions reflect the value of virtual resources. If any unexpected changes happen, the mobile instances intimate the cloud infrastructure and the user through alarm. Using signaled base method malware are detected with high accuracy and short duration. This generally detects the existing malware but couldn't able to identify the newly injected malware. Vaccine application cannot detect the new malware.

Cloud infrastructure connects the number of virtual instances when the malware is accepted. It sends to the entire cloud infrastructure. In order to resolve this problem host data are detected in the virtual instance and network are detected in the cloud infrastructure.

There are two types of mobile cloud contacts creation and non-creation. Creation contacts directly with the mobile users and non-creation contacts by manipulating the background jobs.

2.1 Role of Hypervisor

A hypervisor is a software program which runs the virtual machines. Once the hypervisor is installed on the physical device, it splits the nodes into right and non-rights. Virtual instances executes in non-right platforms. In order to monitor, the virtual instance, there is a bridge applications installed in the virtual mobile instance. This agent based programs supervises

2.2 Types of Mobile Users

Individual Users: Users are classified into three categories normal users, advanced users and developers based on their requirements.

Normal Users: Users are interested in gaming services provided by cloud providers and they access cloud through 3G/4G or Wi-Fi.

Advanced users: Users from private organization may use cloud for their office work. They access cloud services via office Wi-Fi or 3G/4G for simulation work.

Developers: Frequent changes in cloud are necessary for developers; they may use all kind of services provided by cloud.

Office Workers: We categorize office workers as staff in a main office, Staff in branches and agents based on the information they used.

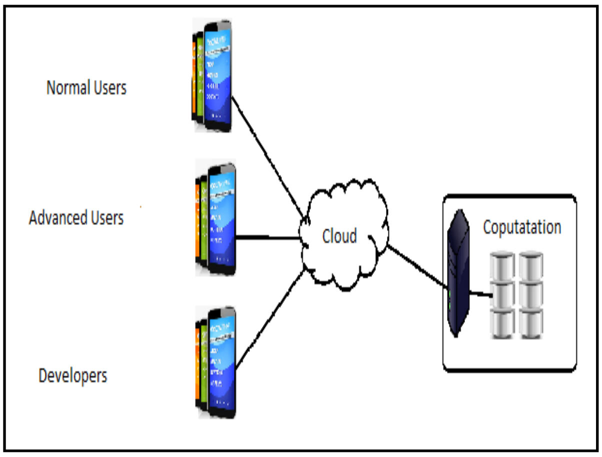

Fig 2: Types of cloud users

Staff in a Main Office: Mobile office system is installed in the main office which can be used by the employees.

Staff in Branch Offices: User needs to have a static mobile environment where they can access system from the branch office to the head office.

Agents: People work with the company to develop a project may use mobile office system.

3. IMPLEMENTING SECURITY ON MOBILE PRIVATE CLOUD

Most of the company wants to have a control over the mobile devices when it is provided by the company or by BYOD (Bring your own device). Mobile Device Management (MDM) with rigid deployment, and stable visibility and control that spans in mobile devices, real documents and the application. Actually this MDM supports all the latest mobile devices including apple iPhone, blackberry, kindle fire, windows phone.

3.1 Security Aspects and the Possible Situations of Attacks

Using the machine learning algorithm, certain features are extracted from the hardware devices like CPU, network utilization, memory were all monitored and malwares are detected using the mobile application .It determines the behavior of the mobile devices while surfing the internet, texting ,making calls and can able to detect the behavior of the device.

3.2 Fault Detection in Mobile Cloud

It tracks the performance of the machine and raises an alarm to found the fault. FDMC is faster than brute-force algorithm. In cloud infrastructure one machine is to play a vital role in mobile cloud called Monitor. Entities are $E_{1,}$ E_2,…….En. Each machine can have the own data partition I_{i} , test points are sent by P_0 it read from the disk.

At any moment of time $P_{0,}$ maintain a current list of t, observation time O_k found. Initially O_K is empty the new Observation time is updated and receive from the entity E_1, E_2,…….En. The monitor to maintain the cut-off threshold C it initially set to infinitive and sequentially increase the value.

Once O_K changes, it set to the least value in O_K and sends it to the entire machine in the cloud. In the CHECK mode to test the block of data read from the memory based on local dataset it trim the points when the current threshold C_i is less than it send the test point to next machine in the ring. The machine P_i maintain threshold C_i it has receive from the monitor $P_{0.}$

Algorithm: CHECK ()

```
Procedure CHECK ()
Begin
For all blocks of data in $I_i$ do
c ← getNextBlock($I_i$);
For all points $b \in B$ do
$N_k(b)$   ∅   ←
For all points $x \in I_i$ do
For $b \in B$, $b \neq x$ do
If $r_{b <} c_i$ then
remove b from B
For $b \in B$ do
Send (b, $N_k(b)$,$r_b$)to machine $P_{i+1}$
```

3.3 Unusual Behavior in Cloud Infrastructure

There is lots of interruption for cloud services. The proposed design can find the anonymous or malicious behavior in the cloud infrastructure. The interruption detection system (IDS) manages the problems in the host interruption detection system (HIDS) and network Interruption detection system. This study doesn't provide how the malicious program is detected. This architecture doesn't display virtualization of each node, but it has the impact in the performance of cloud computing.

Mobile Cloud Computing Group

Number of mobile devices is combined to form a cloud computing group where a larger task is delegated to different mobile devices to make the job done in a shorter period of time and combination of mobile atmosphere.

3.4 Enrolling Mobile Devices

Just by selecting the MDM services and by configuring the device, the particular devices get enrolled. The enrollments request can be obtained using various means (i.e.) by email communication or by SMS or by a custom universal resource locator

Authentication should be provided based on the service provided and the employee designation. By leveraging the existing authentication the services can integrated with the enterprise system .Mobile apps expose lots of personal information.

- Securing mobile devices
- By introducing the passcode policies, certain level of security can be reached
- By strongly enforcing the encryption standards
- Identifying the rooted devices
- Stolen devices should be locked so that unauthorized access can be prevented

Geo-Fencing is a software program which allows system admin to induce a program whenever there is enter or exit condition of the boundaries which is determined by administrator, an automatic intimation or alert is sent. So the company admin can set up boundaries and whenever the mobile is beyond the boundaries, he can disable the device, which is in the private cloud environment.

Evaluation – Gathering behavior data: Test bed is implemented to validate the methodology and architecture. Xen hypervisor is installed on each physical node. Virtual images are created are created using the kernel .Linux gingerbread 2.36 is used and port is mirrored for each physical node.

4. CONCLUSIONS

In the virtual cloud instance abnormal behaviors can be detected using signature based algorithm along with FDMC algorithm so that it finds the nearest neighboring node. Hence all the mobile devices can be checked whether it is affected by malicious program in the cloud.

REFERENCES

[1]. Taehyun 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" 2012 IEEE/IFIP 3rd Workshop on Cloud Management (CloudMan)

[2]. Kanishka Bhaduri, Kamalika Das, Bryan L. Matthews "Detecting Abnormal Machine Characteristics in Cloud Infrastructures"

[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.

BIOGRAPHIES

Currently Pursuing Master of Engineering Degree in Knowledge Institute of Technology Area of interest includes Mobile computing and cloud computing

Currently Pursuing Master of Engineering Degree in Knowledge Institute of Technology Area of interest includes wireless sensor network and cloud computing.

Currently Pursuing Master of Engineering Degree in Knowledge Institute of Technology Area of interest includes cloud computing, big data and mobile cloud.