Providing Cloud Services Over Mobile Cloud Data

Sruthi Tammana#[1], Sri Rashmi Matta#[2], Dr.S.Satyanarayana#[3]

Department of Computer Science and Engineering, Student, K L University, Vaddeswaram, Andhra Pradesh ,India

Department of Computer Science and Engineering, Associate Professor, K L University, Vaddeswaram, Andhra Pradesh, India[3]

Abstract-

In mobile cloud computing, mobile devices can rely on cloud computing and information storage resource to perform computationally intensive operations such as searching, data mining, and multimedia processing. In addition to providing traditional computation services, mobile cloud also enhances the operation of traditional ad hoc network by treating mobile devices as service nodes, e.g sensing services. The sensed information, such as location coordinates, health related information, should be processed and stored in a secure fashion to protect user's privacy in the cloud. To this end, we present a new mobile cloud data processing framework through trust management and private data isolation. Finally, an implementation pilot for improving teenagers driving safety, which is called Focus Drive, is presented to demonstrate the solution.

Keywords*: *Mobile Computing, Mobile cloud infrastructure, Mobile Cloud Service, Malware Detection, RF Algorithm

I. INTRODUCTION

Mobile cloud computing provide some application which have been introduced recently with mobile services having more communication and higher flexibility. We have defined a new method that mobile cloud instances through the mobile infrastructure. There is a drawback where there are threatening problems related to security issues that are present on the mobile cloud instance. Here we solved the problem by introducing mobile services and by using signature based applications. We proposed a methodology to detect the malware through some malicious application within the source content and to validate it, we installed the application through by differential application and detecting virus by the RF Machine learning algorithm that are aroused during the installation of the malicious applications and changing to cloud-based mobile services with more usability and higher efficiency.

II. EXISTING SYSTEM

Generally the normal mobile devices which are present now are defined though while through abnormal detection over mobile cloud service. Most of the applications which are detected through advanced procedure that is signature based method which can detect with high spatial time and efficiency. There is a limitation to this abnormal detection where the modified or new malware introduced. Therefore mobile cloud services should be provided only to detect malicious programs and should prohibit them when using mobile cloud instances ex: vaccine applications which are introduced on mobile cloud instances. If the malware is present on the mobile cloud instance then it is delivered through the mobile cloud infrastructure for detection on the mobile vaccine applications and it happens when monitoring normal behavior over the mobile cloud infrastructure.

III. PROPOSED SYSTEM

Here we instigate on the mobile cloud service detection in mobile cloud infrastructure. There is a signature-based vaccine applications can deliver on virtual mobile instances to detect malware, it makes a substantial instances and advanced for users to install vaccine software by force when those instances are provided as a service. Detection over the mobile cloud service plays a major role which can address those problems by observing difficulties in the cloud infrastructure. To achieve this, we design a monitoring architecture using both the host and network data. Using monitored data, abnormal behavior is detected by applying a machine learning algorithm. To validate our proposal, we have taken a methodology for mobile cloud infrastructure, intentionally installed malicious programs on several virtual mobile instances, and thus successfully detected some applications within abnormal behavior detection through the mobile cloud instances within the service architecture.

A)Mobile Cloud Architecture:

The mobile cloud service which are provided through the installation of mobile devices in cloud infrastructure. The service which is provided means that users connect to virtual mobile instances with their mobile devices and detect on mobile cloud instances. The they have introduced some resources that are applied that is CPU, Memory than it uses some application which have roles to play differently than current applications .Some mobile cloud service providers which are detected through and connect easily on infrastructure which abnormal the behavior through the mobile virtual cloud instances and existing on mobile cloud devices. We propose a mobile cloud instance through the combined form of mobile cloud computing infrastructure and accessing through the resources for current environment.

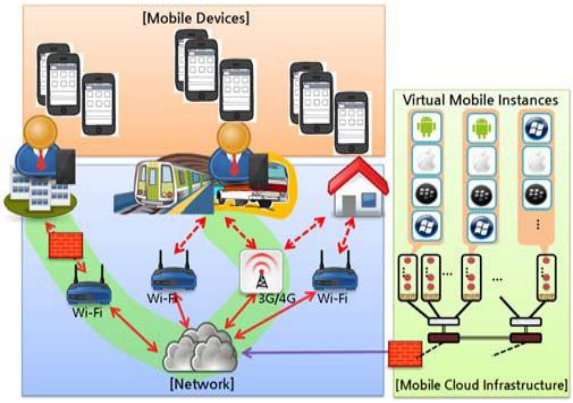

Fig. 1 Mobile Cloud Architecture

B)Mobile Cloud Service Description:

Mobile Cloud Service providers can distribute mobile applications which can connect through the mobile cloud infrastructure to view and interact with the virtual mobile instances. Here we used mobile computing concept which is used for characterization for the purposeful content to describe mobile cloud service architecture. The service scenarios are to detect security threats on mobile cloud infrastructure because they include users, mobile applications. Here mobile computing plays a key role to explain the characterization of mobile computing devices. The proposed mobile cloud service provides virtual mobile instances through the combination of a mobile environment and cloud computing. Some of virtual mobile instances that are present are accessed through some various vaccine applications which is limitation over the proposed methodology. Cloud service providers detect through some of the mechanism which are existing computing resources through achieved detection over various services provided through the mobile cloud.

C)Malware Detection:

Here in the methodology we have introduced signature based method to detect abnormal behavior for that purpose we have taken a 'Gold Miner' malware applications to get abnormal data that provides service in our mobile cloud infrastructure. We tried to install the applications to run on the network that detects abnormal behavior and ran on two hosts , where it have coordinated of particular location and mobile identifiers and sends information present on the server. The malware that is modified cannot be detected when it is applied on the mobile cloud instances which functions on the same behavior through mobile cloud instances which are used to detect malware. When abnormal data is taken and introduce in some of the applications that enters as virus when applied to the external object.

D)Algorithm Implementation:

We used the 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 depicts the dataset that sis formed by combining with position replacement in the training set. In our methodology we used malware detection which have been introduced for some of the applications it explains about the security threats for the existing applications on mobile cloud instances. It generates based on the malicious software that is installed on the mobile cloud services. In our proposed system we detect the normal behaviour of introducing signature based method. But this method is not applied for some of modified cloud instances and new malware which is unknown to the cloud service scenarios explained about the mobile cloud services i.e. vaccine applications so it is better to cause on future proposals. If malware is present on the

instance it is applied on the other mobile cloud service provider which is present on the same host and it also benefits for detecting malicious programs and the abnormal data to be monitored through some usage and enhance it for future applications. The main analysis is taken for each mobile cloud instance over virtual applications.

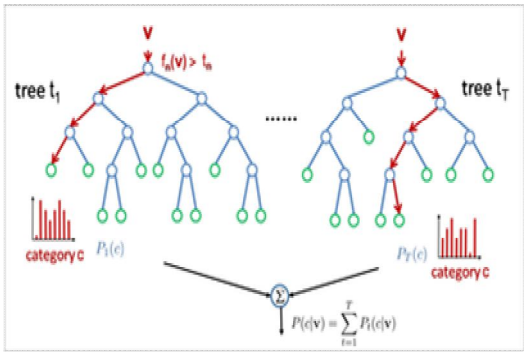

Fig. 2 Example of a sample rf algorithm

IV. CONCLUSION

In this paper, we discussed about the mobile cloud service where security is one of the problem. As a feasible solution of detecting the security threats we proposed a behavior based on the malware detection methodology of monitoring both virtual mobile instances and network data that is present in the given environment. Our solution is better able to detect new modified able instances than signature based methods. The detection methodology is based on machine learning algorithm which is used for determining real time network traffic and hosts that are managed through the information that is passed on the server. In our testing this methodology correctly improves the existing malicious applications and injected into mobile cloud. For future work we will introduce more additional features to detect the abnormal behavior and gather more additional types of sample malware which measures performance of our proposed monitoring architecture. We consider the other monitoring features in order to improve the accuracy and affectivity of using machine learning algorithms and providing mobile cloud services through mobile cloud infrastructure.

REFERENCES

[1] C. Dwork, "The Differential Privacy Frontier Extended Abstact,"Proc. 6th Theory of Cryptography,Springer,2009.

[2] White, Mark "Machine Learning-lecture Slides, Fall 2005.

[3] E. Naone, "The Slow-Motion Internet," Technology Rev.Apr. 2011;

[4] 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.

[5] E. E. Marinelli, "Hyrax: cloud computing on mobile devices using MapRecuce", a Mater Thesis, CMU-CS-09-164, Carnegie Mellon University, September, 2009 which is available in Url:http://reportsarchive.adm.cs.cmu.edu/anon/2009/CMU-CS-09-164.pdf.

[6] H. Dee, D. Hogg, Detecting inexplicable behaviour, in: British Machine Vision Conference, 2004, pp. 477–486.

[7] A. Dempster, N. Laird, D. Rubin, Maximum-likelihood from incomplete data via the EM algorithm, Journal of the Royal Statistical Society B 39 (1977) 1–38

[8] Z. Zhou, D. Huang, Efficient and Secure Data Storage Operations for Mobile Cloud Computing, IACR Cryptology ePrint Archive: 185 (2011).

[9] Distributed Intrusion Detection in Clouds Using Mobile Agents, 2009 Third International Conference on Advanced Engineering Computing and Applications in Sciences.