Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 11, November-2016

Cloud-based Intrusion Detection and Response Mechanism for Smartphones

Ms. Himadriba Jhala
PG Student
CSE Department
B. H. Gardi College of Engineering & Technology
Rajkot, Gujarat, India

***Abstract* — Smartphones are widely used across the world so it is becoming soft target for attackers. Smartphones are more used than personal computers. Nowadays, online shopping is becoming trend for all as well as people save their browsing data, contacts, gallery etc. in smartphone so that we have to concern about all types of data. Smartphones are less in processing power, storage and battery usage. So we propose cloud based intrusion detection and response mechanism for smartphones to overcome the issue of less storage and power and to detect misbehavior activity.**

***Index Terms* — Cloud Computing, DoS Attack, Intrusion Detection System, Intrusion Response System, SNORT, Smartphones**

I. INTRODUCTION

As we place more and more information and rely on smartphones, they become soft targets for information and identify theft as well as denial of service attacks (e.g., battery exhaustion). The major problem with the Intrusion Detection Systems which is developed for mobiles are basically based on the general computer and network technologies [1]. Due to the openness and programmability of Android, it makes smartphones more vulnerable to various malicious attacks, such as Trojan horses, worms, mobile botnets, and so on [2]. The cloud computing provides virtualized resources to the customers using various technologies, for example, Web services, virtualization and multi-tenancy [3]. As far as mobile is concerned we have limited memory and processing power that's why we need to use virtualization of cloud.

II. CLOUD COMPUTING

According to the U.S. Government's National Institute of Standards and Technology (NIST), cloud computing is a "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [4]. Cloud computing is a complex infrastructure of software, hardware, processing, and storage that is available as a service. Cloud computing offers immediate access to large numbers of the world's most sophisticated supercomputers and their corresponding processing power, interconnected at various locations around the world, proffering speed in the tens of trillions of computations per second. Cloud computing seems to offer some incredible benefits for communicators: the availability of an incredible array of software applications, access to lightning-quick processing power, unlimited storage, and the ability to easily share and process information [5].

III. TYPES OF CLOUD

There are mainly four types of cloud computing model, they are also called deployment models of cloud.

They are listed below:
Private Cloud
Public Cloud
Community Cloud
Hybrid Cloud

Public cloud:
In public clouds, multiple customers share the computing resources provided by a single service provider, Customers can quickly access these resources, and only pay for the operating resources [6].

Fig. 1: Public Cloud [7]

Private cloud:
In the private cloud, computing resources are used and controlled by a private enterprise. It's generally deployed in the enterprise's data center and managed by internal personnel or service provider [6].

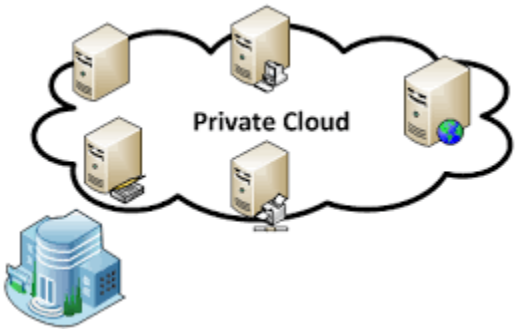

Fig. 2: Private Cloud [7]

Community cloud:
Several organizations jointly construct and share the same cloud infrastructure as well as policies, requirements, values, and concerns [6].

Fig. 3: Community Cloud [7]

Hybrid cloud:
A third type can be hybrid cloud that is typical combination of public and private cloud. It enables the enterprise to running state-steady workload in the private cloud, and asking the public cloud for intensive computing resources when peak workload occurs, then return if no longer needed [6].

Fig. 4: Hybrid Cloud [7]

IV. SERVICES OF CLOUD

Cloud computing is not limited to specific data centers it can be widely used by virtualization also.
There are three implementation styles of cloud computing services.

They are listed below:
SaaS (Software as a Service)
PaaS (Platform as a Service)
IaaS (Infrastructure as a Service)

SaaS:
Service provider provides software services in the cloud. User access these services as software and do his work without installing the same in the local machine [8].

PaaS:
Platform as a Service allows users to use cloud computing for developing any application using development kit provided by cloud computing. Users are not required to install development kit on local machine, he can use installed software or development kit in cloud computing to develop any program [8].

IaaS:
Infrastructure as a Service enables us to install and execute the software. Here, users can gain access to virtualized server. IaaS targets operating systems, hardware, CPUs and embedded systems, networks and storage [8].

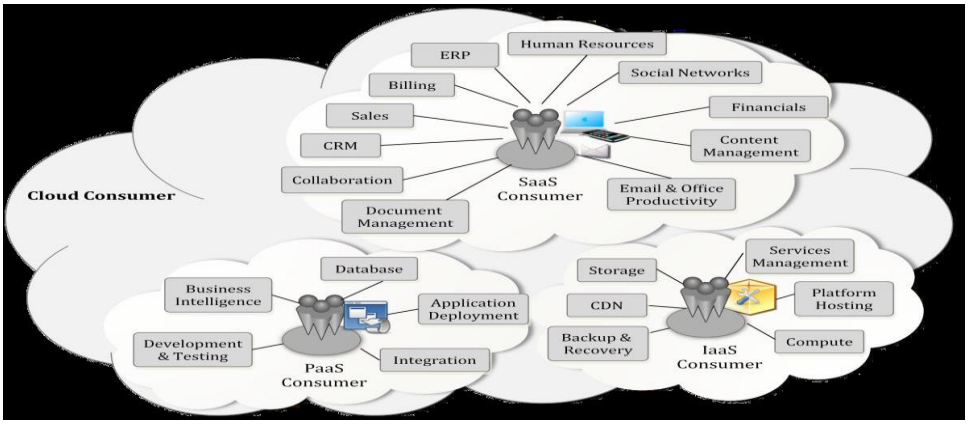

Fig. 5: Hybrid Cloud [9]

V. NEED FOR CYBER SECURITY OF SMARTPHONES

Recent Smartphone security study shows that the mobile operating systems that are being targeted by malware, Trojan and viruses has significantly increased. As per the report released by Kaspersky, the highest number of attack is attempted on Android, attracting a whopping 98.05% of known malware [10]. To protect smartphones in the same way as desktop-PC same security algorithms are required to be used. But these algorithms are highly resource consuming and can be complex too, so they cannot be executed on such smartphone as they are constrained by power, computational and storage limitations [11].

VI. RELATED WORK

There are lot of researchers have been contributing ideas to improve security system for smartphones to enhance intrusion detection system and intrusion response system. Some researchers have provided their own algorithm, mechanism, tool while others have improved technologies, algorithms of current system.

Manish Kumar and Dr. Hanumanthappa [1] propose a cloud based Intrusion Detection System for smartphones to overcome the issues of smartphone resource constraints and to detect any misbehavior or anomalous activity effectively. It consists of a cloud-based service which would allow users to install a light-weight agent on their Smartphone and register to an online cloud-service by specifying their operating system, applications installed on their phone and other relevant information about their device. Afterwards, this specific Smartphone is emulated in a virtual machine on the cloud using a proxy which duplicates the incoming traffic to the device and then forwards the traffic to the emulation platform, where detection is performed.

Fangfang Yuan, Lidong Zhai, Yanan Cao and Li Guo [2] proposed an intrusion detection system for detecting anomaly on Android smartphones. The intrusion detection system continuously monitors and collects the information of smartphone under normal conditions and attack state. It extracts various features obtained from the Android system, such as the network traffic of smartphones, battery consumption, CPU usage, the amount of running processes and so on. Then, it applies Bayes Classifying Algorithm to determine whether there is an invasion.

Amir Houmansadr, Saman A. Zonouz, and Robin Berthier [11] propose a cloud based smartphone-specific intrusion detection and response engine, which continuously performs an in-depth forensics analysis on the smartphone to detect any misbehavior. In case a misbehavior is detected, the proposed engine decides upon and takes optimal response actions to thwart the ongoing attacks. Despite the computational and storage resource limitations in smartphone devices, the engine can perform a complete and in-depth analysis on the smartphone, since all the investigations are carried out on an emulated device in a cloud environment.

Sahil Sakhala, Kshitij Khakurdikar [12] propose a cloud based intrusion detection and response system for detection of anomaly in smartphones that will provide continuous in-depth forensic analysis to detect any misbehavior in network.

Rohit S. Khune and J. Thangakumar [13] propose a cloud based intrusion detection and recovery system for Android smart mobile phones that provides continuous in-depth forensic analysis to detect any misbehavior in network. The mechanism performs analysis on the virtualized and synchronized replica of an actual device in the cloud environment. The analysis on the emulated device includes running multiple detection engines in parallel, memory scanners and system call anomaly detection that generate responses in event of attack. The responses are instructs to mobile agent installed on the device to take essential actions and perform recovery of device if needed.

Asaf Shabtai, Uri Kanonov, Yuval Elovici, Chanan Glezer, Yael Weiss [14] proposed framework realizes a Host-based Malware Detection System that continuously monitors various features and events obtained from the mobile device and then applies Machine Learning anomaly detectors to classify the collected data as normal (benign) or abnormal (malicious). Since no malicious applications are yet available for Android, we developed four malicious applications, and evaluated Andromaly's ability to detect new malware based on samples of known malware. We evaluated several combinations of anomaly detection algorithms, feature selection method and the number of top features in order to find the combination that yields the best performance in detecting new malware on Android.

Namitha Jacob [15] proposing a methodology where an intrusion and detection process is defined in the cloud and it detects the corrupted files in web server. It checks the properties of content in server based on algorithm and an alert message will be given to the smart phone users. Since the application is built in cloud any number of users can download this application from cloud. Call blocking and sms blocking is provided through this application. To validate our methodology, we injected malicious programs into our mobile cloud test bed and used a machine learning algorithm to detect the abnormal behavior that arose from these programs.

VII. INTRUSION DETECTION AND RESPONSE SYSTEM

Intrusion detection systems (IDSs) are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions [12].

IDS plays a role in incident handling processes by performing detection, analysis, producing alerts and also execution of counter measures. IDS also act as a security tools to identify illegitimate users, attacks and vulnerabilities that could compromise security of a resource and the proper functioning of computer systems [12].

The intrusion response decides upon the best countermeasure actions and sends it to a non-intrusive software agent in the device, which is in charge of only carrying out the received actions [11].

VIII. PROPOSED WORK

Most important thing for IDS/IRS is Intrusion Detection, if detection is correct you can do the response. If detection is not correct, your response will not work properly. So need to stress more on Detection Techniques.

As far as Mobile is concern, we have limited memory, power and processing. If you read the IDS implementation technique, majority of them require significant memory and power and that's why the general IDS architecture, which is built for Host or Network will not suite for Smartphones.

So we need to move IDS processing out of the mobile phone and that is why the idea is to use Cloud support.

We proposed Snort tool for detecting Intrusion, Metasploit for generating malicious traffic or payload, it is required for generating attack. We need to create the virtual setup to generate attack on mobile from any system so that system will be consider as attacker. This work can be done on SaaS (Software as a Service) layer of cloud and we need to generate DoS (Denial of Service) attack for better result in detection. We have to configure an IDS. All the communication between mobile and Attacker system should pass through IDS. Our IDS should detect the malicious event. After this detection, response of IDS can be shown by graph which we can say that intrusion response mechanism. Now further this setup has to be scaled up to Cloud, which we can show using virtualization of cloud or hypothetically.

IX. CONCLUSION

The objective of this paper is to provide basic idea of intrusion detection and response mechanism for smartphones using cloud architecture. This system can be used to provide security and tolerance to resource limited mobile phone devices. If any intrusion or malware found then the system will take corresponding response actions to handle the threats. This system will work on the SaaS (Software as a Service) layer hence it will be developed at low cost and efficient in work. We approached use of DoS (Denial of Service) attack which is best suited for SaaS. This system uses lightweight resources and keeps phone free from viruses and malware.

X. REFERENCES

[1] Manish Kumar, Dr. M. Hanumanthappa, "Cloud-based Intrusion Detection Architecture for Smartphones," IEEE, 2015.

[2] Fangfang Yuan, Lidong Zhai, Yanan Cao and Li Guo, "Research of Intrusion Detection System on Android," IEEE, 2013.

[3] Mazhar Ali, Samee U. Khan, Athanasios V. Vasilakos, "Security in cloud computing: Opportunities and challenges", Elsevier, 2015.

[4] Irena Bojanova, Augustine Samba, "Analysis of Cloud Computing Delivery Architecture Models", International Conference on Advanced Information Networking and Applications, 2011.

[5] Rich Maggiani, "Cloud Computing Is Changing How We Communicate", IEEE, 2009.

[6] Jianfeng Yang, Zhibin Chen, "Cloud Computing Research and Security Issues", IEEE, 2010.

[7] Ms. Shubhangi Ashok Kolte, Prof. P E Ajmire, "A Survey - Cloud Computing", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 4, April 2016.

[8] Sameer Rajan, Apurva Jairath, "Cloud Computing: The Fifth generation of Computing", International Conference on Communication Systems and Network Technologies, 2011.

[9] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf , "NIST Cloud Computing Reference Architecture ", NIST Publication, September 2011.

[10] Christian Funk, Maria Garnaeva Kaspersky Security Bulletin 2013, Overall Statistics for 2013, December 10, 2013.

[11] Amir Houmansadr, Saman A. Zonouz, and Robin Berthier, "A Cloud-based Intrusion Detection and Response System for Mobile Phones," IEEE, 2011.

[12] Sahil Sakhala, Kshitij Khakurdikar, "Anomaly Detection For Smart Phones Using Cloud-Based Intrusion Detection and Response Systems", International Journal & Magazine of Engineering, Technology, Management and Research, ISSN No: - 2320-3706, Jan 2014.

[13] Rohit S. Khune and J. Thangakumar "A Cloud-Based Intrusion Detection System for Android Smartphones" International Conference on Radar, Communication and Computing (ICRCC), 2012.

[14] Asaf Shabtai, Uri Kanonov, Yuval Elovici, Chanan Glezer, and Yael Weiss. "Andromaly: a behavioral malware detection framework for android devices". Journal of Intelligent Information Systems, pages 1–30, 2011. 10.1007/s10844-010- 0148-x.

[15] Namitha Jacob, "Intrusion Detection in Cloud for Smart Phones," IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013.