International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.82.034

Analysis of Cloud Security through Honeypots

ShrutiPuri
M.Tech Research Scholar
Computer Science & Engg.
Amritsar College of Engineering and Technology,Amritsar

Manoj Agnihotri
Assistant Professor in C.S.E Deptt.
Amritsar College of Engineering and Technology, Amritsar

Abstract : Cloud computing provide access to large pools of high end resources through variety of interfacres that are similar to the approach in HPC computing resource management. Cloud computing is gaining popularity in recent years as easy of provising the utilities and services to the end users as per cost basis. The end user does not need to run the programs that require high end resources to their local computer, rather they shift the computing and execution of it on the cloud platoform. Protecting the cloud resources from ever increasing cyber threats is of great importance in these days. The intruders are entering in the cloud network and current state of art intrusion detection systems are only capable to detect known atatck as so called they are highly dependent on the rule sets in their databases. Most of the current network based intrusion detection systems are purely rule based hence only capable to handle the known set of attacks.In this work, we present the exploit gathering and its analysis through integration of varous security tools and techniques such as network intrusion detection systems and also honeypot based mechanims that help us to enhance the security in cloud infrastructures. The honeypots are designed and placed in a cloud network that help us to gather the unknown as well as known incidents occured in cloud computing. The purpose of this paper is to highlight the importance of honeypot in protection of cloud based infrastructures. The prood of concept of the system are demonstrated through experiments.

KEYWORDS : Honeypots, Intrusion detection system, threats, Malwares, Cloud infrastructures, Unknown attacks

I. INTRODUCTİON

In the context of cloud computing, the on-demand access to the shared list of resources such as server, storage, applications and services are provided to the end user with minimal intrruption and intervention from service providers [[1]. These set of resources are connected over the global virtual world known as Internet. The end user only need a PC and Internet connectivity to access these resources.

In the current internet world, the cloud computing infrastructure and its usage is increasing exponential manner. Even though there is a limited companies who are dominating in the domain of cloud computing technology, the growth of it could only be seen in a rapid manner. As per the prediction in [2], the spending on cloud infrastructures will increase by 46%. According to [2], enterprises are predicting that in 2015 they will increase their spending on cloud computing by 46%. The prediction was made in [3], 92% of all work load will be cloud-borne.

However the increase use of these infrastructure is also attracting another domain that of cyber attacks. There are various studies documented that depicted the rise of security incidents that go undetected by the current security mechanism in place and number of such successful breaches are increasing. When we look at the statistics, the number of detected cyber attack incidents reported in 2014 was 48% more than 2013. As per the security threat report of Symantec [26], in 2015 the number of zero-day vulnerabilities discovered more than doubled to 54 that 125 % more than the previous year.

The growth of cyber attacks incidents is getting even worse due to current trend of more number of interconnected devices and cloud based services that make a complex network with myriad of interdependencies. The threat risks propagate rapidly in such kind of computing environment.

To defend such security attacks, there are various conventional approaches in place that include setting of perimeter security in-depth, and these are also deployed by the cloud service providers. The unified security appliances has gained the popularity in last decades as it allows the monitoring and management of multiple ranges of security tools through single interface. These security mechanisms such as firewall, Intrusion detection systems, UTMs and anti-viruses are usually based on passive defense system that is so called rule sets based detection approach. They have limited detection capabilities which is purely depend upon the crated rule sets aka signatures, hence there are incapable to protect the network and assets in a network.

The report mentioned in [6] about the cloud related threat in the last quarter of 2016 and observed that monthly organization reached 18.4 % increase as compared to the last year. The cloud security breaches are described

in[7-8] those target most of the cloud computing enviornment. The iCloud hack leaked the photo of celerebirities- including Kate Upton and Jennifer Lawrence -- to the public. Due to a number of celebrities falling prey to the hack, hysteria ensued over the security of cloud.

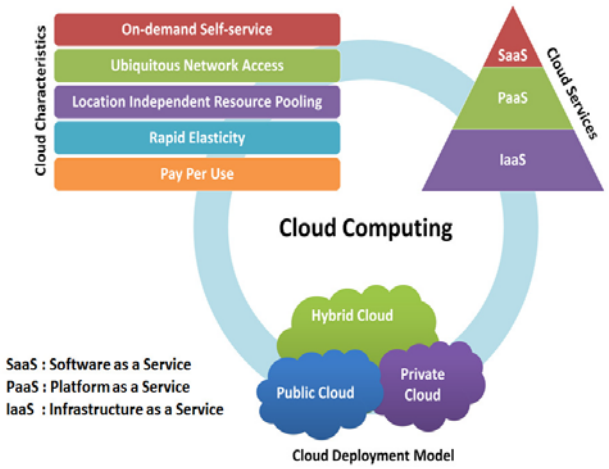

Figure 1: Cloud Computing Models

Given the sophisticated nature of cyber attacks and their growing tendency towards evolving in a phased approach, one has to think outside the box and investigate unconventional approaches to prevent, detect, and recover from cyber attacks [27]. One approach is to integrate active defense mechanisms in cyber security frameworks that allow the monitoring of attacks in a controlled setting with the intent to learn attack patterns and prepare appropriate counter measures to determine them. An example of such mechanism is honeypot, which is a system, either isolated production system or emulated one that is configured to be deliberately vulnerable, with the ultimate goal to be probed and exploited by attackers. If data is collected and analyzed it could contribute in detecting imminent attacks, dry runs of attacks, or multi-phased attacks. It is by no means a trivial task. However the analysis of attack patterns may be beneficial to the protection of network assets.

II. RELATED WORK

The cloud computing in not a new thing, it is a matter of fact that cloud computing concept originates since 1950s [14], when the mainframe computers made available to the schools and corporations. In addition to it, the on-demand concept of cloud computing concept went back to the time sharing model in the era of 1960s [9]. Thereby many of the security issues related to cloud computing are quite similar to the internet world. Due to the adoption of technology Virtualization, the service based architecture of cloud computing has been evolved and malware detection is becoming the necessity for such service based infrastructures. The author in [10] introduced the malware detection in cloud computing by introducing the “CloudAV- antivirus scanner” for cloud networks. Many authors targeted the security issues in cloud computing and its structure as well as some detection system for cloud network such as Static analysis, Signature Based pattern matching and dynamic analysis detection systems. The author Oberheide [10] proposed in his dissertation “CloudAV- N Version Antivirus system in the network” that is a new model for AV deployments and scanning of suspicious files in the cloud. The approach introduced by the researcher was novel approach which outperform the traditional host based anti-virus scanner capabilities that include better detection capabilities of malicious software with improved deployable and manageable retrospective detection. Use a production implementation and real-world deployment of the Cloud AV platform.

In addition to the above Schmidt, [11], proposed the combined approach for malware detection and kernel rootkit prevention in a virtualized cloud computing environments, and all running binaries in virtual instance are intercepted and submitted to one or more analysis engines. Besides a complete check against a signature database, lives introspection of all system calls is performed to detect yet unknown exploits or malware.

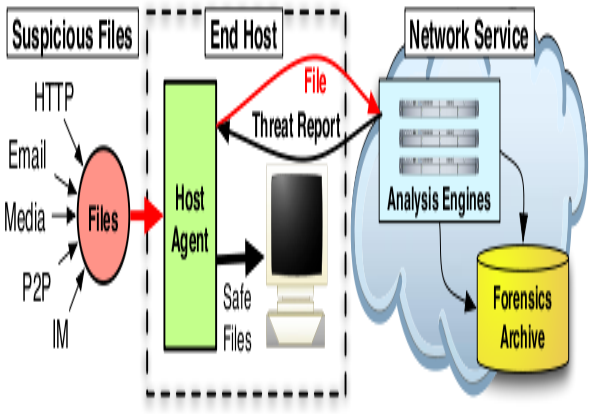

Figure 2. Work flow of cloud computing security system

As mentioned in L. Spitzner [28], the honeypot is a security resources whose value lies in being probed, attacked and compromised. The ultimate goal of putting the honeypot is to lure the attackers so that the activities of the attacker can be captured and logged and further analyzed for handling the incidents.
A generic model of a honeypot comprises of the following components [29]: honeypot system (vulnerable system resource that is expected to become the target of attacks), firewall, monitoring unit (monitor the network traffic in the entire system and report potential violations), alert unit (generates alerts while violations occur), and logging unit (storage facility of all kinds of generated logs from various sources). There are several honeypot taxonomies that classify honeypots based on various criteria (or classes) [30-32]. The basic taxonomy categorizes honeypots using two broad independent classes: the type of the honeypot resource (server or client) and the level of interaction (low, high, hybrid).

III. PROPOSED SYSTEM

3.1.1 Baselining the cloud infrastructure

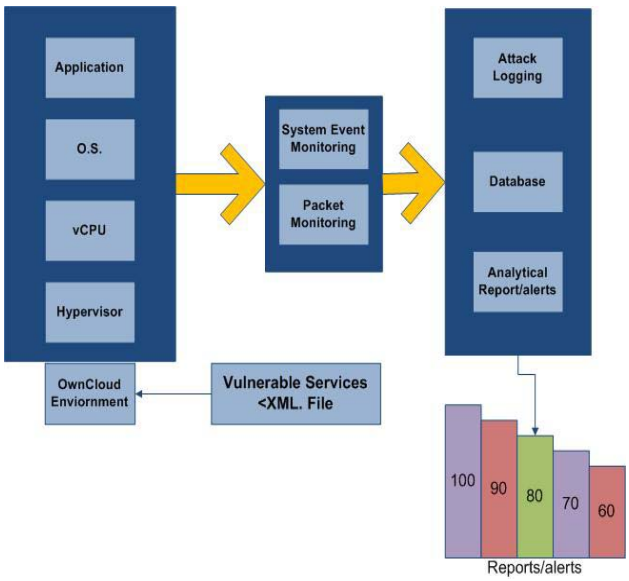

Figure 3: System Design

The proposed baselining of implemented system is depicted in figure 4. For creation and establishment of cloud infrastructure, the OwnCloud is being used that is open source desktop based cloud software. The Hypervisor of the OwnCloud has been used for hosting the applications in virtualized cloud network. The vulnerablie list of services are ported into OwnCloud in a standard <XML> file as blueprint of the deployed vulnerabilities. The popular list of vulnerable services and associated ports are identified and incoporated them into a blueprint file for easily deployments. Normally the end user is connected to the cloud infrastructures through a PC with internet connectivity. For this few set of services are always requires such as HTTP, SSH etc, the set of such

services are build through a blueprint file and embedd into the cloud network. This is a sort of lightweight low interaction honeypot application that is embedded into the cloud infrastructure.
After the incorporation of honeypot application, the system level and network level logging and capturing are enabled for monitoring and logging of any suscpecious files in a cloud infrastructure. In parallel, the network level logging are also enabled to log the packet communications for the OwnCloud Desktop cloud.
The details of captured data has been stored into a database for further applying the data analytics of the atatck data. The crucial part here is which algorithm should be applied to analysed the logged activities. The details of working flowchart of attack data capturing and analysis is depcited in figure 4.

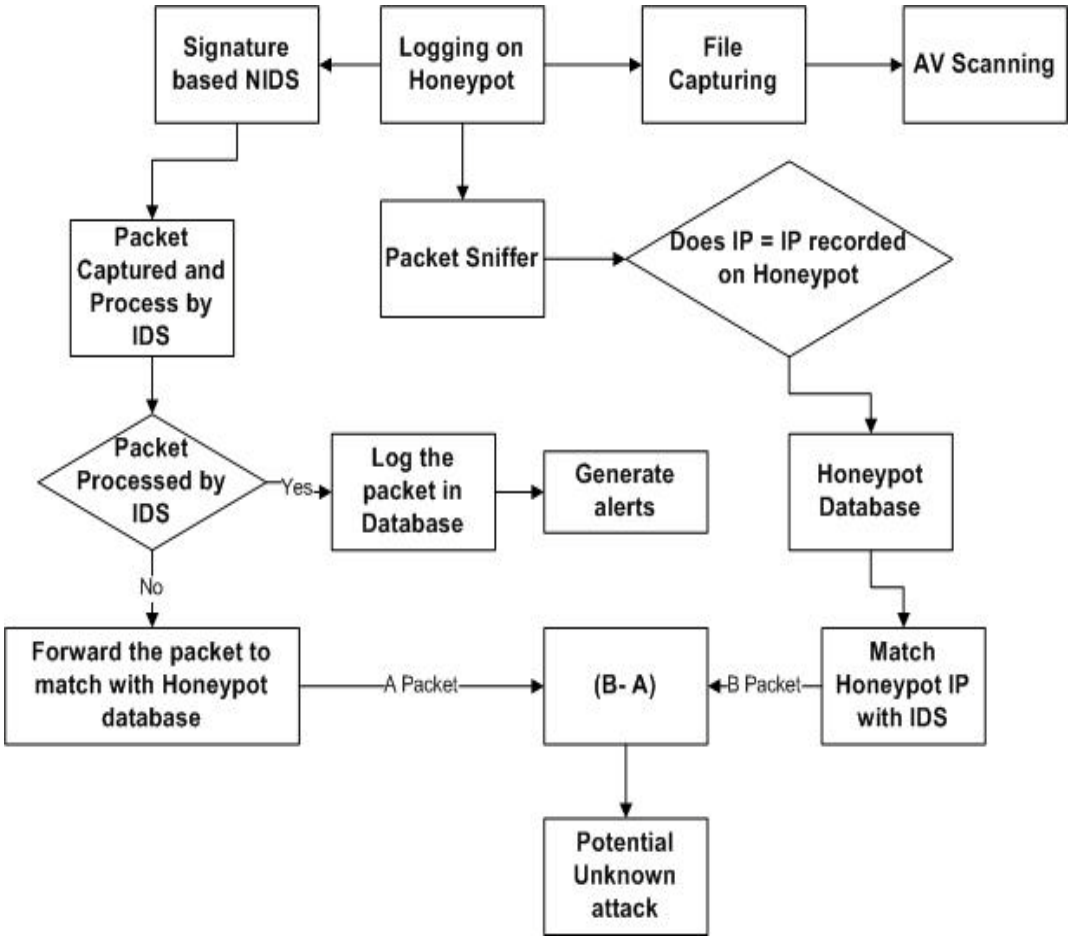

Figure 4: Flowchart of Implementation

IV. METHODOLOGY

Attack plan may involve different attack strategies, such as port scanning, password guessing, malware download, buffer overflow, and each will leave some trace in log. Based on our preliminary study, hacker applies different attack strategies at different stages, for example, applying port scan to find a vulnerable machine and then exploiting it. Once he gets control of the first one, it starts exploiting/attacking the next one or the planned target machine. Therefore, each piece of an alert or audit trace may represent a step of an on-going attack. Inferring multiple types of logs in a time frame may observe stages of an attack plan. The cloud setup creation and expoit gathering workflow is depicted in figure 5. The first of the our implementation is ceration of cloud setup, for that we have adopted owncloud platpform that is open source cloud platform and big benefit is that open source virtual machine is available. User can compile and install the necessary packages as per the requirement and also the readily available VDI image may be used for direct implementation. Below are the refined steps to compile the OwnCloud as cloud package on a Ubuntu linux machine. The hardware for this implementatis in used as Dell PC with 64-bit architecture, 8GB RAM, 200GB Hard disk.

http://dx.doi.org/10.21172/ijiet.82.034

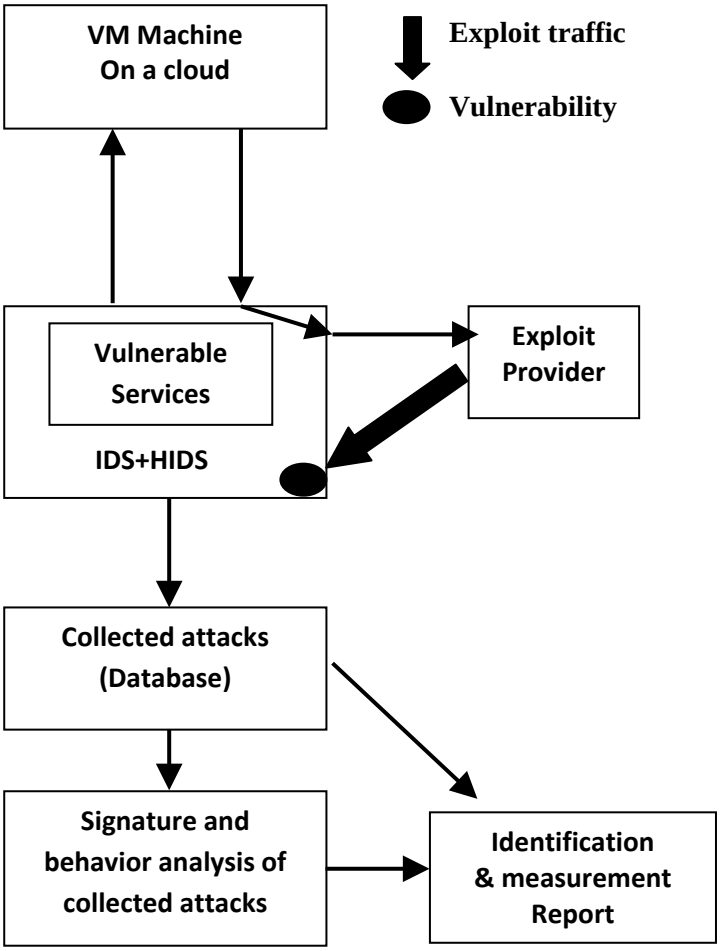

Figure 5: System Design

V. EXPERİMENTAL RESULTS AND USE CASES

Tools and libraries Used:

- OwnCloud [15]
- TCPDUMP[16]
- Libpcap[17]

Step 1: Test the network connectivity from base machine to VM machine

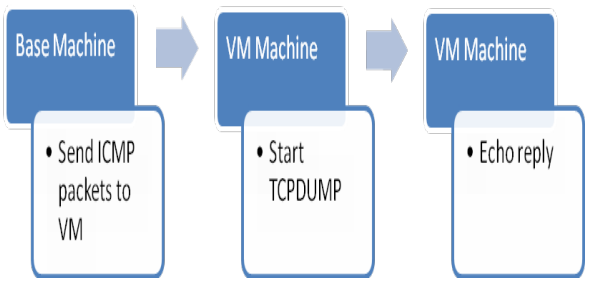

Figure 6: Setup of Base and VM machine

- Send ICMP packets to VM machine, the VM machine will respond with the echo reply packets

http://dx.doi.org/10.21172/ijiet.82.034

Step 2: Development of shell script for automated packet capturing in cloud environment.

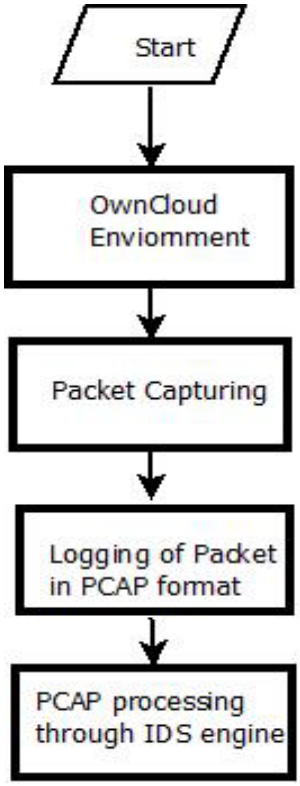

Figure 7: Packet capturing and processing flow

- Start the packet capturing engine
- Read the captured files through tcpdump and IDS engine

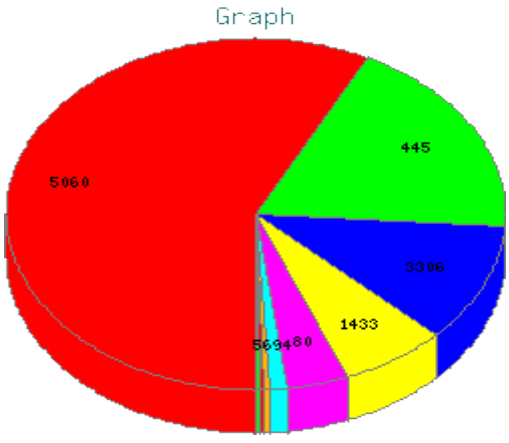

Figure 8: Destination Ports targeted by the attacker

VI. CONCLUSİON AND FUTURE WORK

The cloud computing is a growing area with inclusion of advanced technologies and very well adopted by the end users but it is constantly under the threats due to weak security placed in the cloud infrastructure. In this research, we have highlighted the need and requirements of security scanner to protect and prevent the user's data hosted in the cloud infrastructure. Normally, the cloud resources are more vulnrable then the normal end user PC because the resources are hosted over the internet which is always a public network and very prone to attacks.

This research highlighted the implementation of proactive security mechanism in the form lightweight low interaction honeypot to handle the communication from end user PC to the cloud network. The setting up and deployable solution of honeypot is being implemented on the cloud infrastructure and attack data are captured and communication from end user PC to the cloud network. The setting up and deployable solution of honeypot is being implemented on the cloud infrastructure and attack data are captured and logged into a database for further analysis. The novelity of this approach is the baselining process of honeypot application that is easily deployable in the cloud infrastructure.
The core benefit of the proposed approach are:

- It can detect known and unknown attacks
- Controlled use of honeypot sensors through baselining process for easy incorporation and deployments for gathering of attacks.

The implementation of high interaction honeypot .as real operating system and resources that will simulate the complete resource of a cloud infrastructure is proposed with inclusion of console for easy visilization of attacks for future work

BİBLİOGRAPHY AND REFERENCES

[1] Grance, T., Mell, P.: The nist definition of cloud computing. National Institute of Standards & Technology (NIST) (2009). URL http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf
[2] PwC, "The global state of information security survey 2015," PwC, Tech. Rep., 2014.
[3] https://www.forbes.com/sites/joemckendrick/2016/12/22/my-one-big-fat-cloud-computing-prediction-for-2017/#423c19806a86
[4] https://www.cloudendure.com/blog/5-cloud-experts-predict-cloud-computing-trends-2017/
[5] https://www.helpnetsecurity.com/2016/03/01/top-12-cloud-computing-threats-in-2016/
[6] https://www.skyhighnetworks.com/cloud-computing-trends-2016/
[7] http://searchcloudcomputing.techtarget.com/feature/Cloud-security-breaches-still-the-stuff-of-IT-nightmares
[8] http://searchcloudcomputing.techtarget.com/podcast/iCloud-hack-hoopla-ensues-but-cloud-blame-misplaced
[9] Chen, Z. & Yoon, J. "IT auditing to assure a secure cloud computing", (2010). [Online]: http://doi.ieeecomputersociety.orgezproxy.umuc.edu/10.1109/SERVICES.2010.118.
[10] J. Oberheide, E. Cooke, and F. Jahanian "CloudAV: N-Version Antivirus in the Network Cloud", In Proceedings of the 17th USENIX Security Symposium (Security'08). San Jose, CA, 2008.
[11] Jon Oberheide, Evan Cooke and Farnam Jahanian "Cloud N-Version Antivirus in the Network Cloud",Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor, MI 48109 (2007).
[12] Matthias Schmidt, Lars Baumg Artner, Pablo Graubner, David Bock and Bernd Freisleben "Malware Detection and Kernel Rootkit Prevention in Cloud Computing Environments." University of Marburg, Germany (2011).
[13] K. Murad, S. Shirazi, Y. Zikria, and I. Nassar, "Evading Virus Detection Using Code Obfuscation" in Future Generation Information Technology, vol. 6485 of Lecture Notes in Computer Science, pp. 394–401, Springer Berlin , Heidelberg, 2010
[14] Safaa Salam Hatem et.al, Malware Detection in Cloud Computing, *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol.* 5, *No.* 4, *2014*
[15] https://owncloud.org/
[16] www.tcpdump.org/tcpdump_man.html
[17] yuba.stanford.edu/~casado/pcap/section1.html
[18] Bhavesh Borisaniya et.al, Incorporating Honeypot for Intrusion Detection in Cloud Infrastructure.
[19] Nitin Chandra S.R, Cloud Security using Honeypot Systems, International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 1 ISSN 2229-5518
[20] Eman Al Awadhi et.al, Assessing the Security of the Cloud Environment, 2013 IEEE GCC Conference and exhibition, November 17-20, Doha, Qatar
[21] Andreas Fischer et al, CloudIDEA: A Malware Defense Architecture for Cloud Data Centers
[22] Dolgikh, A., Birnbaum, Z., Chen, Y., Skormin, V.: Behavioral modeling for suspicious process detection in cloud computing environments. In: IEEE 14th Int. Conf. on Mobile Data Management (MDM). vol. 2, pp. 177–181 (June 2013)
[23] Gionta, J., Azab, A., Enck, W., Ning, P., Zhang, X.: Seer: practical memory virus scanning as a service. In: Proceedings of the 30th Annual Computer Security Applications Conference. pp. 186–195. ACM (2014)
[24] K. Murad, S. Shirazi, Y. Zikria, and I. Nassar, "Evading Virus Detection Using Code Obfuscation" in Future Generation Information Technology, vol. 6485 of Lecture Notes in Computer Science, pp. 394–401, Springer Berlin , Heidelberg, 2010
[25] http://www.networkcomputing.com/network-security/cloud-malware-threat/1806517482
[26] www.symantec.com/security-center/threat-report/
[27] Defense-Systems-Magazine. Iarpa wants an early warning system for cyber attacks. [Online]. Available: http://defensesystems.com/articles/2015/07/24/iarpa-cause-cyber-early-warning-system.aspx
[28] L. Spitzner, *Honeypots: Tracking Hackers*. Addison Wesley, 2002.
[29] R. Joshi and A. Sardana, *Honeypots A New Paradigm to Information*n*Security*. CRC Press, 2011.
[30] P. K. Christian Seifert, Ian Welch, "Taxonomy of honeypots," Technical Report CS-TR-06/12, Victoria University of Wellington, School of Mathematical and Computing Sciences, Tech. Rep., June 2006.
[31] C. Polska, "Proactive detection of security incidents: Honeypots," ENISA, Tech. Rep., 2012.
[32] N. Provos and T. Holz, *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Addison-Wesley Professional, 2007.