http://dx.doi.org/10.21172/ijiet.81.030

Review: A Study on Malware Detection in Cloud Network Targeting Cloud Infrastructures

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 is accepted by many companies to put their resources such as server, storage and applications on the cloud network somewhere on internet. The end user's data is placed on cloud infrastructures with minimal cost which makes cloud computing is one of the promising and growing technology. In an abstract terms, the cloud computing technology enable the users to access the large infrastructures and resources for high speed computing through a different middleware that are similar to existing Grid and HPC computing. These type of systems provide the environment to host the scalable applications and these also gained the popularity over the past decades. But instead of providing the shared platform to the users, the cloud network is prone to various security risks such as malwares infections, distributed denial of service attacks, SQL injection and even more complicated attacks in the form of botnet zombies. In this paper, we present a study of security issues and infection propagation in cloud network. However detection capabilities of tradition host based anti-virus is limited and these software fails to detect many threats and complexity of latest attacks are increasing which evade the traditional security mechanisms. In this paper, malware detection and research work on these techniques are presented to get the internals of cloud security and putting the advance malware detection techniques to protect the cloud infrastructures. In a cloud network, the resources are provided to the end user in the form of virtual machines, which make them vulnerable to malware exploits, VM Escape based attacks and even distributed denial of service attacks of the resources hosted over the cloud network.

KEYWORDS: cloud computing, malwares, anti-virus, cloud security, databases, virtualization.

I. INTRODUCTİON

Over the past years, the cloud computing is becoming a dominant technology and widely adopted by the companies and user communities. The kind of flexibility and scalability provided by the Cloud Service Provides enable to more and more users of the technology. Instead of increasing use of cloud computing technology, it is very prone to various security risks. The CSPs can secure their infrastructures by installing the latest security tool over it but what about the end user's data. How they should be ensured that their data hosted over the cloud somewhere over the internet is secure. The possibilities are that the security attacks can occur when the user's is accessing its data. The malware can be planted and inserted into cloud virtual machine which is accessed by the end user. In the current technological world, the security system is very important for any organization to protect the data and any kind of information that are kept in their computer. The intruder is able to access the organization's computer and control it in some way to view and access the resources Many of us are aware about how to use the computer but not aware how to protect it. The same is applicable to cloud network, users and companies are excited about the cloud technology but most of them do not aware about what kind of security system to be installed to protect the user's data and other resources. Cloud security is really an emerging domain of computer security, it cover the broad set of security in the form of policies, technologies and controls deployed that protect the data, applications and the associated infrastructure of cloud computing.

It is widely accepted by the researcher and commercial partners that detection of malicious software is a complex problem. The ever-increasing scale of tools, exploit kits to launch the malicious program making more difficult for current security mechanism to detect and prevent them. The anti-virus software is one of the majorly used tools for detection and prevention of unwanted software, however detection of more sophisticated attacks and modern malwares make a challenging task for them to detect and develop the signatures for every class of new malwares.

As per the recent report published in [1],discuss about the top 10 security concern pertain to cloud computing which include- data breaches, Hijacking of accounts, Insider threat, Malware injection, abusing cloud services, insecure APIs, DDoS attacks, Insufficient Due Diligence, shared vulnerabilities, and data loss.

In this paper, we present a study and assessment of current security mechanism in the context of cloud security and adaption of new tools and techniques for malware detection in cloud network.

II. CLOUD SECURİTY

2.1 CLOUD SECURİTY FUNDAMENTALS

One of the unique characteristics of cloud environment is that it is distributed in nature, the cloud service provider may allocate and de-allocate the resource based on the availability of them at that particular moment of time. For computation of huge amount of data and its processing, a cloud service provider may use the free resources at that time. It provides great flexibility in terms of computation and resource requirements by the users, however it exposes the end user’s data over the entire network which is major concern of serious security threats pertains to cloud infrastructures and user’s data hosted over these resources.

In the context of cloud computing, the Cloud Service Provider provides the resources via the internet through usage of virtualization technologies that has self-replication capabilities. The resources in the form of virtual machines from different organization are hosted on a same physical server that optimize the cost and efficiencies of the cloud services. By shifting of organizational critical application and sensitive data over the cloud network, the CSP must ensure the basic security and protection of user’s data. For this most of the CSP implant the various security engines such as PKI, Intrusion detection and prevention system to prevent and reduce any security risk within the organization.

One of the strength of the cloud environment is its distributed nature of the renounces. For huge and rapid processing of the data, a CSP may use resources which are available at that time of operation. This feature exposes the user data over entire network which may cause serious security threat. To overcome this issue, an intrusion detection system (IDS) mechanism is generally preferred in the cloud paradigm. Broadly security in cloud network can be divided in four categories- Cryptography approach, virtualization security, infrastructure security and cloud storage security.

Authors in [21] discussed the details about the Intrusion detection system and its roles in the computer security. In present scenario, the security is implemented in any organizational network through utilizing the firewall, IDS, anti-virus and malware detection capabilities in a single bundle as UTM that is Unified Threat Management framework. The research presented in [23] used the Bayesian network for intrusion detection, further construction of decision network based on exact attack characteristic is presented.

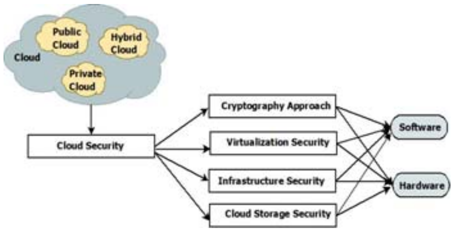

Figure 1: Basic Cloud Security

2.2 MALWARE DETECTİON TECHNİQUES APPLİED İN CLOUD COMPUTİNG

In this section we discuss the research and implemented approached for cloud security that lead to detection of malwares infection propagation in a broad way. The following table depict the approached that are majorly discussed by various researchers and even functioning in various cloud infrastructures.Cloud services are prominent within the private, public and commercial domains. Many of these services are expected to bealways on and have a critical nature; therefore, security and resilience are increasingly important aspects. In order to remain resilient, acloud needs to possess the ability to react not only to known threats, but also to new challenges that target cloud infrastructures

. Table 1: Research in Cloud Security

Sr.No.	Research Paper	Descriptions	Detection Techniques	Applicability
1	Watson et.al [3], "Malware Detection in Cloud Computing Infrastructures", IEEE TRANSACTIONS-2016	In this paper, the author introduced and discussed an anamolay based detection mechanim applicable to cloud infrastructure. Further the noval detection technique in the form of support Vector Machine(SVM) by utilizing the network and system levels features of the cloud node. They had demonstrated the detection accuracy as more than 90 percent whilst detecting various types of malware andDoS attacks.	Support vector machine based anomaly based intrusion detection by adoption network and system events of VMs	Cloud based Virtulization (VM) through hypervisor
2	Andreas Fischer et.al[4], "CloudIDEA:A Malware Defense Architecture for Cloud Data Centers", , Volume 9415 of the series Lecture Notes in Computer Science pp 594-611, 2015	In this research, the author presented the a malware defense architecture in the form of security as service model for defensive security against malwares in cloud infrastructure. In this paper, the two appraches are applied – lightweight detection and heavyweight detection. In case of lightweight detection, the on demand isolation of VM are performed if intrusion is detected in a VM through system events, Then in case of heavyweight detection- in depth, complete analysis of VM is being performed through VMI (Virtual Machine introspection). The major contribution of this research is a dynamic decision engine that makes on-demand decision on how to handle the suspicious events considering cost-efficiency and quality-of-service constraints.	Virtual Machine Introspection through LIbVMI library	VM introspection of Cloud Virtual Machine
3	Prachi Deshpande et.al[5], Indian Institute of Technology Roorkee "Security Threats in Cloud	The author in this research presented t he detailed analysis and then categorization of various security threats that were occured on cloud	Signature based intrusion detection and prevention	Cloud infrastructure based security.

	Computing”, IEEE Xplore 2015	network. In this mainly the SNORT IDS detection is presented which is open source and widely accpeted intrusion detection and prevention system (IDPS).	system	
4	ByungRae Cha et.al [6], “Security Tactics for Secured Cloud Computing Resources”, IEEE Xplore 2013	In this research, the multi-stage anomaly detector and honeypot placed in outside of the cloud network along with attribute-based access control in inside of cloud computing for secured cloud computing resource .	Anomaly based detection with inclusion of attribute based access control.	Cloud infrastructure Security
5	Harald Gjermundrød et.al[7], Department of Computer Science School of Sciences and Engineering University of Nicosia Nicosia, Cyprus, “CloudHoneyCY - An Integrated Honeypot Framework for Cloud Infrastructures”- ACM-2015	In this paper, the focus of the discussion is on how honeypots, a non-traditional security technology not adequately represented in the protection mechanisms pool, could be deployed in the cloud to allow the analysis of attack patterns. To be more specific, CloudHoneyCY is presented, an open-source framework that supports a collection of low-interaction and high interaction honeypots deployed in the cloud infrastructure with the purpose of collecting and analyzing attack data that aids in constructing attack profiles.	Proactive based security using Honeypot for intrusion detection in cloud network.	Cloud Infrastructure Security
6	Eman Al Awadhi et.al[8], “Assessing the Security of the Cloud Environment”, IEEE Xplore-2013	In this paper, the researcher assesed and studied the security of a typical cloud enviornment. The secuirty of the cloud is assessed through deployment and running of Dionaea honeypots	Proactive Security through Honeypots	Public Cloud Network provided by CSP
7	Jordi Ros-Giraltet.al [9]“Scalable Cyber-Security for Terabit Cloud Computing”, USA, IEEE-HPEC	The author addressed the scalability of cyber security using a cloud infrastructure in two ways 1) power and performance efficiency 2) Degree of of relevent information detected. A framework was presented which include building blocks as -forwarders, analyzers and grounds. A new queuing policy is introduced which is TED- tail early detection to drop the packets in a proactive way.	Proactive approach and early tail detection of mal packets	Private Cloud that is implemented to demonstrate the capabilties of framework.
8	Ming Zhao et.al[10], Florida International University, School of Computing and Information Sciences, Miami, FL “Multi-level VM Replication based	The author addresses the security issues in VM through virtual machine replication once there is malicious event detected. Further this research introduced the noval approach of multi-level VM replication technique that uses VM clones to provide protection	VM Replication techniques is used.	Hybrid cloud, capabilities are introduced both on private and public cloud infrastructure

	Survivability for Mission-critical Cloud Computing", IEEE-2015	againt the critical applications and improve their survivability against the malicious event detected in the VM machine.		
9	Safaa Salam Hatem et.al[11], "Malware Detection in Cloud Computing", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 4, 2014	In this paper, the researcher presented the combination of static and dymanic approaches for detection of malicious files and unwanted softwares instead of relying only on Anti-virus engine, the detection is based on mulitple engines deployed as a service in a cloud enviornment.	Static and Dynamic Detection based approach for detection of malwares in cloud infrastructure	Public cloud by hosting the application as public use.
10	CLOUD SECURITY REPORT HONEYPOT FINDINGS-2014[12]	In this report, alert logic a commercial partner deployed the set of honeypot sensors in public cloud enviornment/infrastructures at geo—ocations and observed the attacks and how the attacks are varied geographically.	Proctive based approach	Public Cloud Infrastructure
11	Stephen Brown et.al[13], "Honeypots in the Cloud", University of Wisconsin – Madison, December 19, 2012	The combination of honeypot sensors such as Dionaea, Kippo and amun are deployed on public cloud as a cloud instances and observed the attack patterns. In this paper, the author observed that by deploying the honeypot sensors as a service model in cloud infrastructure, most of the attack trafic origionated from US and China. In the end, the author conclude that Dionaea and Kippo- low interaction honeypots are more suitable for cloud enviornment.	Honeypot based approach that is proactive technique for detection of attacks	Public Cloud
12	Nithin Chandra S.R, Madhuri T.M [14], "Cloud Security using Honeypot Systems"	The author in this paper assess the cloud security through honeypot implementation. This is sort of study paper which depict the usage of honeypot in cloud security.	Honeypot- a proactive approach for cloud security	Public cloud
13	Kumar Shridhar, Nikhil Gautam[15], "A Prevention of DDos Attacks in Cloud Using Honeypot", International Journal of Science and Research (IJSR)	In this research, the author presented tha prevention of DDoS attacks by deployment of honeypot sensors.	Proactive approach to handle the DDoS attacks	Public Cloud

14	M Balamurugan et.al [16], “Honeypot as a Service in Cloud”, International Conference on Web Services Computing” (ICWSC) 2011, Proceedings published by International Journal of Computer Applications® (IJCA)	At first, the author highlighted that resources in a cloud enviornment are more vulnerable as they are connected together. Thereby the hacker can easily take control of the centralized control unit to monitor the entire network. Honeypot running in a cloud enviornment helps to trap the hackers and it can be provided as service model.	Honeypot based detection approach	Public Cloud

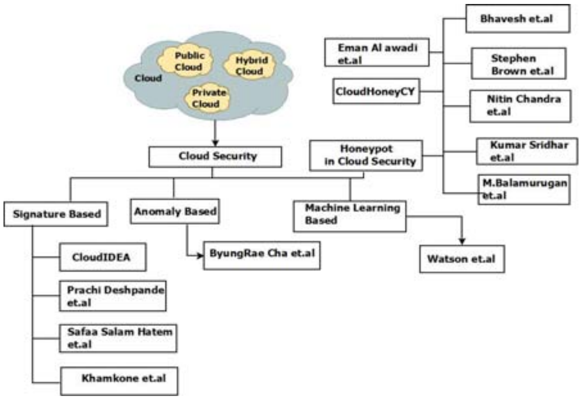

Figure 2: Research in Cloud Security.

III.CONCLUSİON

In current technology, the cloud computing is one of the most growing technology and adopted by the users but it is constantly under the threats because of weak security mechanims placed. In this review, we have highlighted the requirements of security scanner implementations to protect the user’s data hosted in cloud infrastructures. The cloud resource are more vulnerable than the normal PC because these resources are accessed by the user via internet which is always a public network and prone to attacks.

REFERENCES

[1] https://www.incapsula.com/blog/top-10-cloud-security-concerns.html

[2] Microsoft, “Microsoft security intelligence, report”, http://www.microsoft.com/technet/security/default.mspx, July December 2006.

[3] Michael R. Watson, Noor-ul-hassan Shirazi, Angelos K. Marnerides, Malware Detection in Cloud Computing Infrastructures, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 13, NO. 2, MARCH/APRIL 2016

[4] Andreas Fischer et.al, CloudIDEA: “A Malware Defense Architecture” for Cloud Data Centers, OTM 2015 Conferences, Volume 9415 of the series Lecture Notes in Computer Science pp 594-611

[5] N. Kajal, N. Ikram and Prachi, "Security threats in cloud computing," International Conference on Computing, Communication & Automation, Noida, 2015, pp. 691-694.doi: 10.1109/CCAA.2015.7148463

[6] B. Cha and J. Kim, "Security tactics for secured cloud computing resources," The International Conference on Information Networking 2013 (ICOIN), Bangkok, 2013, pp. 473-475.doi: 10.1109/ICOIN.2013.6496425

[7] H. Gjermundrød and I. Dionysiou, "CloudHoneyCY - An Integrated Honeypot Framework for Cloud Infrastructures," 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC), Limassol, 2015, pp. 630-635.

[8] E. A. Awadhi, K. Salah and T. Martin, "Assessing the security of the cloud environment," 2013 7th IEEE GCC Conference and Exhibition (GCC), Doha, 2013, pp. 251-256.doi: 10.1109/IEEEGCC.2013.6705785

[9] Scalable Cyber-Security for Terabit Cloud Computing (Jordi Ros-Giralt, Peter Szilagyi, Richard Lethin), In Supercomputing Conference Companion, Salt Lake City, UT, USA, November, 2012.

[10] M. Zhao, F. D'Ugard, K. A. Kwiat and C. A. Kamhoua, "Multi-level VM replication based survivability for mission-critical cloud computing," 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, 2015, pp. 1351-1356.

[11] Safaa Salam Hatem et.al, Malware Detection in Cloud Computing, (IJACSA). International Journal of Advanced Computer Science.

[12] https://www.alertlogic.com/assets/cloud-security-report/alertlogic-HoneypotFindings2014-infographic.pdf

[13] Stephen Brown et.al, Honeypots in the Cloud, University of Wisconsin – Madison, December 19, 2012

[14] Nithin Chandra S.R, Madhuri T.M, Cloud Security using Honeypot Systems, International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 ISSN 2229-5518

[15] Kumar Shridhar, Nikhil Gautam, "A Prevention of DDos Attacks in Cloud Using Honeypot", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064

[16] M Balamurugan et.al, "Honeypot as a Service in Cloud, International Conference on Web Services Computing" (ICWSC) 2011,Proceedings published by International Journal of Computer Applications® (IJCA)

[17] https://en.wikipedia.org/wiki/File:Cloud_computing.svg

[18] Yunqi Ye, Liangliang Xiao, I-Ling Yen and F. Bastani, "Cloud Storage Design Based on Hybrid of Replication and Data Partitioning," 16th International Conference on Parallel and Distributed Systems, Shanghai, China,2010, pp. 415 – 422, doi: 10.1109/ICPADS.2010.11.

[19] K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B.Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, Vol. 4, No. 1, 2013, pp. 1-13.

[20] A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, "Towards Secure Mobile Cloud Computing: A Survey," Future Generation Computer Systems, Vol. 29, No. 5, 2013, pp. 1278-1299.

[21] Amor, N.B, Benferhat, S, Elouedi, Z.: Naive Bayes vs. "Decision Trees in Intrusion DetectionSystems. In: Proc. ACM Symposium on Applied Computing, New York, pp. 420–424 (2004).

[22] Kruegel, C, Mutz, D, Robertson, W, Valeur, F.: Bayesian Event Classification for IntrusionDetection. In: Proc. 19th Ann. Computer Security Applications Conference, NY, pp. 14–23(2003).

[23] Forrest, S.A. Hofmeyr, S.A, Somayaji, A, T.A. Longstaff.: A Sense of Self for UnixProcesses," In: IEEE Symposium on Security and Privacy, Oakland, pp. 120–128 (1996).

[24] Ye Du, Wang, H, Pang, Y.: A Hidden Markov Models-Based Anomaly Intrusion DetectionMethod. In: Fifth World Congress on Intelligent Control and Automation, Vol 5, pp. 4348–4351 (2004).

[25] Warrender, C, Forrest, S, Pearlmutter.B.: Detecting Intrusions Using System Calls: AlternativeData Models. In: Proc. IEEE Symposium on Security and Privacy, Oakland, CA, pp. 133–145(1999).

[26] E. Alata, V. Nicomette, M. Ka^aniche, M. Dacier, and M. Herrb. Lessons learned from the deployment of a high-interaction honeypot. In Dependable Computing Conference, 2006. EDCC'06. Sixth European, pages 39{46. IEEE, 2006.

[27] M. Balamurugan and B.S.C. Poornima. Honeypot as a service in cloud.

[28] R. Challoo and R. Kotapalli. Detection of botnets using honeypots and p2p botnets. International Journal of Computer Science and Security (IJCSS), 5(5):496, 2011.

[29] E. Cooke, F. Jahanian, and D. McPherson. The zombie roundup: Understanding, detecting, and disrupting botnets. In Proceedings of the USENIX SRUTI Workshop, pages 39{44, 2005.

[30] J. Gobel. Amun: A python honeypot. Universit at Mannheim/Institut f ur Informatik, 2009.