TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 2069 - 2072

Integrated Cloud Data Storage and Attacks Diagnosis Using Big Data

[1]Chaitanya Sai Gajula, [2]D. Mahalakshmi

[1]Student, Department of Computer Science & Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai, Tamilnadu, India-602105
[2]Assistant Professor, Department of Computer Science & Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai, Tamilnadu, India-602105
[1]gajulachaitanyasai@gmail.com, [2]mahalakshmid.sse@saveetha.com

Article Info
Volume 82
Page Number: 2069 - 2072
Publication Issue:
January-February 2020

Article History
Article Received: *14 March 2019*
Revised: *27 May 2019*
Accepted: *16 October 2019*
Publication: *12 January 2020*

Abstract

In existing system, the virtualized infrastructure in cloud computing systems had become an attractive target for the cyber system attackers to launch advanced attacks within the planned systems, novel knowledge primarily based security analytics approach to detection advanced stacks in virtualized infrastructures. Network logs moreover as user logs collected sporadically at the guest virtual machines square measure keep within the hadoop distributed classification system. If any malware commands attacks the network system can gather the science address of aggressor system within the modification method, we are implementing a system establish to spot the network traffic occurred by attackers and identify the attackers World Health Organization is offensive the server. Those science addresses are going to be send to another system which identify the aggressor of shell commands.

Keywords: *Cloud Computing, Security, Storage Data Privacy big data analytics, Suspicion.*

1. Introduction

Now a day's cloud data centres are commencing to be used for a spread of always-on services across all domains. These got to be safe and robust within the face of challenges that embody cyber-attacks still as element failures and mis-structure. However, clouds have characteristics and deep sitting internal operational structures that weaken the employment of ancient detection systems especially vary of valuable properties were offered by the cloud, like the service transparency and adaptability, introduce variety of vulnerabilities that are the result of its underlying virtuality nature. Moreover an implied downside lies with the cloud's external dependency on informatics networks, wherever their flexibility security had been extensively read, but however it still retains a difficulty.

Big data is all-circumferential term for any assemblage of data sets so massive and complicated that it becomes tough to method victimisation ancient processing applications. There are various challenges which includes analysis, capture, duration, search, sharing, storage, transfer, visual image, and privacy violations. Trend to various knowledge sets is because of the extra info derived from analysis of one large set of connected knowledge, as compared to separate smaller sets with an equivalent total quantity of information, permitting correlations to be found to &quote ; spot business trends, stop diseases ,combat crime then on. Thus we are able to implement massive knowledge in our project as a result of each use has schooled info thus we are able to create analysis on this knowledge.

Virtualized infrastructure consists of virtual machines (VMs) which are depending on the software-defined multi instance resources of the hosting hardware. The virtual machine monitor, additionally referred to as hypervisor, sustains, regulates and manages the software-defined multi-instance design. The flexibility to pool totally different computing resources similarly as alter on-demand resource scaling has semiconductor diode to the widespread preparation of virtualized infrastructures as a vital provisioning to cloud computing services. This has created virtualized infrastructures become a beautiful target for cyber attackers to launch attacks for extra-legal

January - February 2020
ISSN: 0193 - 4120 Page No. 2069 - 2072

access. Exploiting the software package vulnerabilities among the hypervisor ASCII text file, refined attacks like Virtualized atmosphere Neglected Operations Manipulation (VENOM) are performed which permit associate aggressor to interrupt out Of a guest VM and get entry to the underlying hypervisor .additionally, attacks like Heartbleed and Shellshock that exploit the vulnerabilities among the software can even be used against the virtualized infrastructure to get login details of the guest VMs and perform attacks starting from privilege step-up to Distributed Denial of Service (DDoS). Existing security approaches to protective virtualized infrastructures typically embrace 2 sorts, particularly malware detection and security analytics. Malware detection typically involves 2 steps, first, observance hooks are placed at totally different points among the virtualized infrastructure, and then regularly-updated attack signature information is employed to work out attack presence. Whereas this enables for a time period detection of attacks, the employment of infatuated signature information makes it liable to zero-day attacks that it's no attack signatures.

2. Literature Survey

[1] Searchable coding is of increasing interest for safeguarding the information privacy in secure searchable cloud storage. During this paper, we tend to investigate the protection of a widely known scientific discipline primitive, namely, public key coding with keyword search (PEKS) that is extremely helpful in several applications of cloud storage. sadly, it's been shown that the normal PEKS framework suffers from associate inherent insecurity known as within keyword guesswork attack (KGA) launched by the malicious server. To deal with this security vulnerability, we tend to propose a brand new PEKS framework named dual-server PEKS (DS-PEKS). As another main contribution, we tend to define a brand new variant of the sleek projective hash functions (SPHFs) said as linear and homomorphic SPHF (LH- SPHF). We tend to then show a generic construction of secure DS-PEKS from LH-SPHF. let's say the practicability of our new framework, we offer associate efficient internal representation of the final framework from a choice Diffie–Hellman-based LH-SPHF and show that it are able to do the sturdy security against within the KGA.

[2]Data sharing is a very important practicality in cloud surroundings. With the appearance of the planet Wide internet and also the emergence of e-commerce applications and social networks, organizations across the planet generate an outsized quantity of information daily. This information would be additional helpful to cooperating organizations if they were ready to share their information. During this article, associate economical methodology is provided to firmly, expeditiously, and flexibly share information with others in cloud computing, however the opposite encrypted files outside the set stay confidential. Secure scientific discipline design and dealing methodology square measure projected during this paper for best services over the cloud.

3. Existing System

Virtualized infrastructure in cloud computing has become an attractive target for cyber attackers to launch advanced attacks. The attackers can easily attack the virtualized infrastructure in cloud computing. The attackers launching the advanced attacks in the cloud. The attackers perform the advanced attacks in the cloud systems and they gain the data in the cloud systems. By this the data can be lasted. A lack of secure connectivity in a hybrid cloud surroundings hinders the version of clouds by way of clinical communities that require scaling-out of the neighborhood infrastructure the use of publicly to be had sources for large-scale experiments.

4. Disadvantages

- More number of attacks were made on cloud server
- Anyone can access the cloud using user's login and password.

5. Proposed System

Big data based security analytics approach on detecting the advanced stacks in virtualized infrastructures systems. Network logs as well as user logs collected regularly from the guest virtual machines are saved at hadoop distributed file system. If any malware commands attacks the network system will gather the IP address of attacker system.

We are implementing a system to identify the network traffic occurred by attackers and identify the attackers who is attacking the server. Those IP address will pass to another system which identify the attacker of shell commands.

6. Advantages

- IP address will block if DDos attack identified
- Check behaviour of user
- Block unauthorized accessing of user
- Integrating big data to block user

7. System Architecture

The expediency of the project is analysed during this section and business setup is place away with an awfully general set up for the project and a few price live. Throughout system inquiry the expediency read on the planned system is to be administered. It can certify the planned system isn't a hassle to the corporate. For expediency analysis, some understanding of the foremost needs for the system is important.

January - February 2020
ISSN: 0193 - 4120 Page No. 2069 - 2072

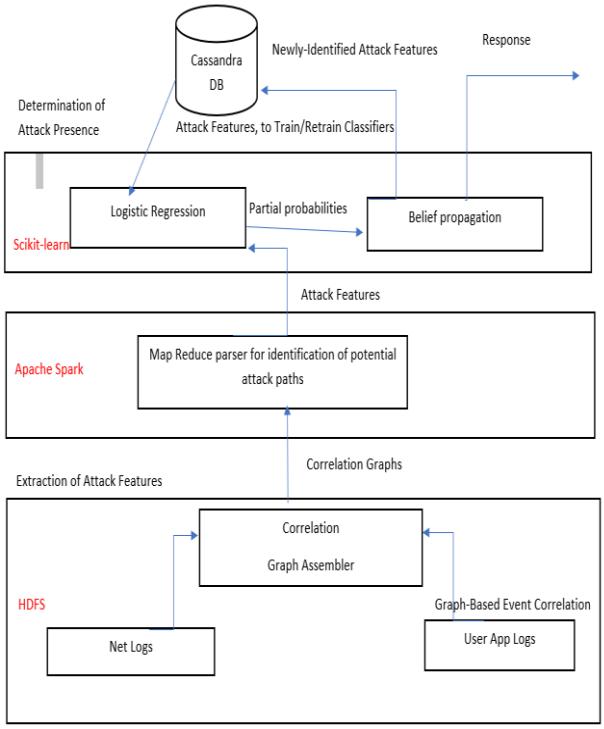

Figure 1: System Architecture

Three key issues worried within the feasibility evaluation are

- COST EFFECTIVE EXPENDIENCY
- TECHNICAL EXPENDIENCY
- OPERATIONAL EXPENDIENCY

8. Result and Conclusion

Thus the project concludes that through this system we identify the attacks and log file separately. In this paper we had shown a web anomaly detection capturing method which can be implemented at the hypervisor degree of the cloud infrastructure. Architecture that was initially defined further explored and which comprises the System Analysis Engine (SAE) and Network Analysis Engine (NAE) components. These exist as sub modules of the architecture's Cloud Resilience Managers (CRMs), which perform detection at the end-system, and in the network respectively. Evaluation was focused on detecting anomalies as produced by a variety of malware strains from the Kelihos and Zeus samples under the formulation of a novelty detector that employs the one-class Support Vector Machine (SVM) algorithm.

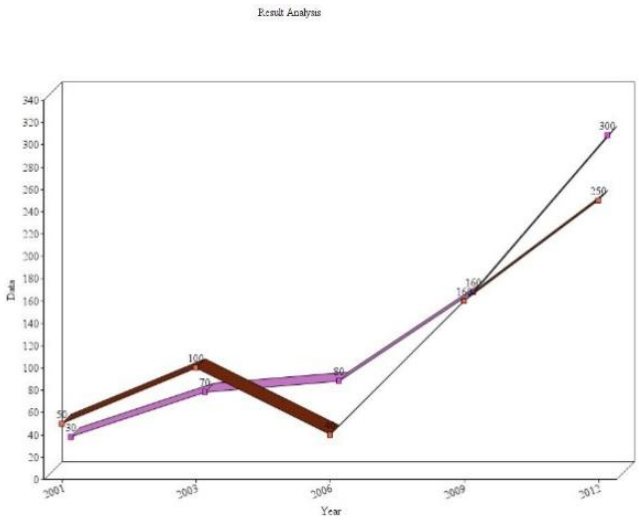

Figure 2: Kelihos and Zeus samples

Moreover, for you to empower the widespread homes of our detection approach we also examine the detection of anomalies via the SAE and NAE in the course of the onset of DDoS attacks.

References:

[1] D. Fisher, "'venom' flaw in virtualization software could lead to VM escapes, data theft," 2015. [Online]. Available: https://threatpost. com/venom-flaw-in-virtualization-software-could-lead-tovm-escapes-data-theft/112772/, accessed on:May 20, 2015.

[2] Z. Durumeric, et al., "The matter of heartbleed," in Proc. Conf. Internet Meas. Conf., 2014, pp. 475–488.

[3] K. Cabaj, K. Grochowski, and P. Gawkowski, "Practical problems of internet threats analyses," in Theory and Engineering of Complex Systems and Dependability. Berlin, Germany: Springer, 2015, pp. 87–96.

[4] J. Oberheide, E. Cooke, and F. Jahanian, "Cloud AV: N-version antivirus in the network cloud," in Proc. USENIX Secur. Symp., 2008, pp. 91–106.

[5] X. Wang, Y. Yang, and Y. Zeng, "Accurate mobile malware detection and classification in the cloud," SpringerPlus, vol. 4, no. 1, pp. 1–23, 2015.

[6] P. K. Chouhan, M. Hagan, G. McWilliams, and S. Sezer, "Network based malware detection within virtualised environments," in Proc. Eur. Conf. Parallel Process., 2014, pp. 335–346.

[7] M. Watson, A. Marnerides, A. Mauthe, D. Hutchison, and N.-ul-H. Shirazi, "Malware detection in cloud computing infrastructures," IEEE Trans. Depend. Secure Comput., vol. 13, no. 2, pp. 192 205, Mar./Apr. 2016.

[8] A. Fattori, A. Lanzi, D. Balzarotti, and E. Kirda, "Hypervisor based malware protection with

January - February 2020
ISSN: 0193 - 4120 Page No. 2069 - 2072

Access Miner," Comput. Secur., vol. 52, pp. 33–50, 2015.

[9] T. Mahmood and U. Afzal, "Security analytics: Big data analytics for cyber security: A review of trends, techniques and tools," in Proc. 2nd Nat. Conf. Inf. Assurance, 2013, pp. 129–134.

[10] C.-T. Lu, A. P. Boedihardjo, and P. Manalwar, "Exploiting efficient data mining techniques to enhance intrusion detection systems," in Proc. IEEE Int. Conf. Inf. Reuse Integr., 2005, pp. 512–517.