IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

IJARSCT

Impact Factor: 6.252

Volume 2, Issue 3, November 2022

Identification of Multiple Attacks in Cloud Environment using Big Data

Dr. Samydurai A[1], Achuthan R[2], Akash K[3], Eber Sheckel E[4]

Associate Professor, Department of Computer Science and Engineering[1]

UG Scholar, Department of Computer Science and Engineering[2,3,4]

SRM Valliammai Engineering College, Chengalpattu, Tamil Nadu, India

Abstract: *Since the Cloud environment is prone to many attacks we are implementing a Big Data based centralized log analysis system to identify the network traffic occurred by attackers through DDOS, SQL Injection, and Brute Force attacks. The log file is automatically transmitted to the centralized cloud server where big data is initiated and uses a tool called Hadoop to process the huge amount of log files that are being sent to big data. If an attacker attacks any files then it will be compared with the attack dataset that is maintained here to detect the attacks that are being used by the attacker. This system also helps in storing the information of all registered users, and their files which get uploaded to the cloud server and downloaded from the server and IP addresses in order to view any attacks that may occur in the future. All this stored information is maintained securely using SQL which is a backend process. Thus we are implementing a system that delivers a very high performance as well as very efficient results in categorizing the attacks. Since the Hadoop tool is being used in the system, this system is able to increase its scalability and achieves a faster detection of attacks like DDOS, SQL Injection, and Brute Force attacks. This system can play a vital role in various organizations to safeguard their privacy. Data integrity, Data confidentiality, and non-repudiation can be achieved by using this system. Finally, we can say that this system avoids any faults that occurred in the previous system that was invented before this.*

Keywords: Brute force attacks, Hadoop, Data Integrity, SQL Injection, DDOS Attacks

REFERENCES

[1]. D. Fisher, "'venom' flawin 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

[2]. on:May 20, 2015.

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

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

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

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

[7]. P. K. Chouhan, M. Hagan, G. McWilliams, and S. Sezer, "Network-based malware detection within virtualized environments," in Proc. Eur. Conf. ParallelProcess., 2014, pp. 335–346.

[8]. 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.

[9]. Fattori, A. Lanzi, D. Balzarotti, and E. Kirda, "Hypervisor based malware protection with Access Miner," Comput. Secur., vol. 52, pp. 33–50, 2015.

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

DOI: 10.48175/IJARSCT-7633

[11]. 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.

[12]. Alexander Tolstoy & et.al.,(2010).Application of Big Data, Fast Data andData Lake Concepts to Information Security Issues

[13]. Hussein T.Mouftah & et.al.,(2010).Big Data Analytics: Security andPrivacy Challenge 13.Karim Abouelmehdi & et.al.,(2020).Big Data Emerging Issues: Hadoop Security and Privacy

[14]. Elisa Bertino & et.al.,(2018). Big Data Security and Privacy

[15]. Azzam Mourad & et.al.,(2018). How to Distribute the Detection Load among Virtual Machines to Maximize the Detection of Distributed Attacks in the Cloud?

[16]. Michael R. Watson & et.al.,(2018).Malware Detection in Cloud Computing Infrastructures

DOI: 10.48175/IJARSCT-7633