ECONSPEAK: A Journal of Advances in Management IT & Social Sciences,
Vol. 13, Issue 04, April 2023 Impact Factor 8.059 ISSN: (2231-4571)
www.skirec.org Email Id: skirec.org@gmail.com

INTRUSION DETECTION SYSTEMS IN CLOUD COMPUTING SYSTEMS: AN OVERVIEW AND ANALYSIS

Agha Urfi Mirza[1], Dr. Anand Kumar[2]

[1,2]Department of Computer Science, Capital University, Koderma (Jharkhand)

ABSTRACT:

The cloud computing paradigm is quickly gaining popularity because it enables customers to obtain services via the Internet on a pay-per-use basis and because it simplifies the process of creating, deploying, and accessing mobile applications. Because of the open and decentralised nature of the cloud, security is currently an essential topic that must be addressed. Large volumes of data are the root cause of the appeal that hackers have. Creating an effective IDS is a work that must be completed immediately. The purpose of this study was to investigate the effectiveness of intrusion detection systems in identifying attacks. In this experimental analysis, a cloud platform was set up using OpenStack, and an IDS was configured to monitor the entire network traffic of the web server that was set up. When a DDoS attack is taking place, the results reveal that Suricata is more effective than Bro and Snort in detecting malicious packets and dropping fewer packets than Bro and Snort sequentially.

Keywords: *Intrusion Detection Systems; Cloud Computing; Distributed Denial of Service*

INTRODUCTION:

Intrusion Detection networks (IDS), are security solutions that, along with other precautions like Communications and data networks may be made more secure by using anti-virus applications, firewalls, and and various access methods for control. Numerous IDS strategies have been put forth in the academic community since the invention of this equipment, but the "Common Intrusion Prevention Framework" (CIDF), and that refers to the "Common Intrusion Identification Framework," is a group of experts that was founded by DARPA[1] in 2019 via the main goal of overseeing and developing a uniform structure in the information security sector (Ugochukwu et al 2019; Tchakoucht&Ezziyyani, 2018). This group has been responsible for some noteworthy work in this area. Integrated into IETF[2] in the year 2000, and the crew suggested a fundamental IDS design according to an analysis of a further four distinct kinds of functioning parts, and after selecting the new abbreviation IDWT[3] (Fig. 1):

[1]Defense Advanced Research Projects Agency

[2]Internet Engineering Task Force

[3]Intrusion Detector Works Team

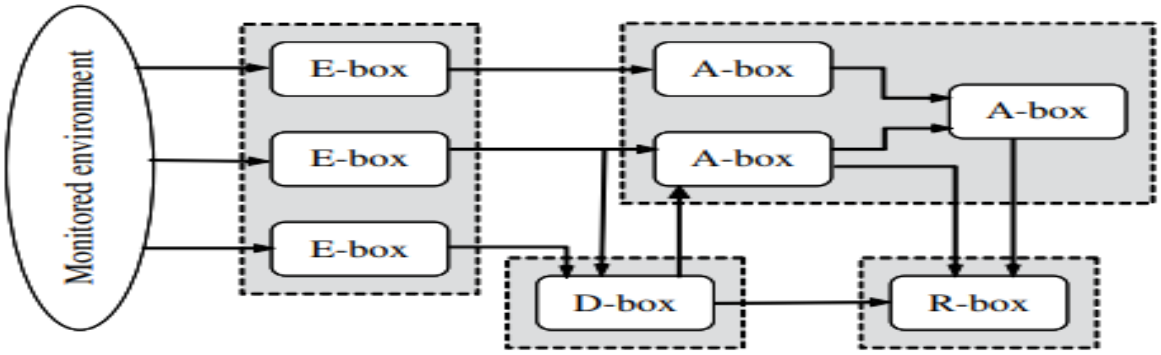

Figure 1: IDS computers' fundamental CIDF configuration (Alzahrani, &Alenazi, 2021)

The previous literatures that pertain to this notion are discussed in greater detail in the next section.

AUTHOR	TECHNOLOGY IMPLEMENTED	METHODOLOGY	RESULTS & FINDINGS
(Li, 2018)	Using large data collection techniques in conjunction with user-based ontology mapping	Big data solution Hadoop makes use of the MapReduce framework. Users may more precisely find knowledge about medical and technical advancements that they are curious about thanks to this design strategy, which centers on a user behaviors semantic model and combines tailored recommendations by combining stated interest and inferred demand.	Offer a big data examination and decision-making solution that is scholarly, thorough, timely, and trustworthy for individualized intelligence advice and smart control over technology and scientific advancements.
(Yan et al., 2019)	Optimization algorithm for unsupervised learning	A CNNRNN model has been built by them. At its heart is the use of clouds. It's a map-re method and return propagation were used. It was	The other methods might be used to verify the effectiveness.

		utilized in validation and refinement procedures that covered the many approaches utilized by the health care industry. To tackle this, big data and cloud computing systems are employed. Gaps in application and projected change have been explored.	
(Wang et al., 2020)	the huge data analysis model that is decentralized and online	The use of big data mining to regulate computer networks is examined. effectively using big data analysis for military computer systems	In order develop internal oversight mechanisms that both constrain and enable one another, to enact and strengthen the company's system of control, and to speak towards options rooted in the present state of the firm, the analysis recommends a novel savvy structure for holistic analysis of business management capabilities.
(Hongsong et al., 2021)	the huge data analysis model that is decentralized and online	In the suggested method, both practical and intangible needs were gathered and tailored towards the big data platform.	use four distinct assault methods. The security concerns are fully classified, and all safety problem's defensive solutions are examined.
(Rana et al., 2022)	Two standard benchmark datasets, namely, NSL-KDD and UNSW-NB15, were used for the simulations.	This paper outlines growing threats to sensitive user data security and offers solutions.	The hybridization method with support vector machine classifier outperforms other methods on the datasets tested.

Table 1: Literature review

METHODOLOGY:

Snort, Suricata, and Bro are the tools that are utilised for the experiments. They are all considered to be network intrusion detection systems, abbreviated IDS for short. Snort has a strong reputation in the business world, and the majority of its users are leaders of networks. The characteristic is that it is single threaded of this programme that is the most inconvenient since it leads to numerous problems and results in the dropping of many packets when Snort is receiving a significant proportion of traffic. It is possible to compare Suricata to Snort. In point of fact, it is compatible with Snort and has the ability to read the log files generated by the latter. In contrast to Snort, Suricata offers multi-threading capability, which makes it possible for the software to take use of advanced multi-core technologies and multiprocessing. This is another one of the program's positive aspects.

RESULTS AND DISCUSSIONS:

The main objective of this work was to effectively identify the distributed denial supply attacks. in order to assess the IDS's efficacy. This set up 10 machines, or clients, which use the OpenStack cloud platform in order each of which has a Python application that launches an attack on a web server. that was specifically built for this objective. Fig. 2 provides a description of the architecture that was utilised for this particular assault scenario. Each server utilises the Ubuntu 14.04 operating system, and each has four virtual CPUs, two gigabytes of RAM, and four gigabytes of hard drive space. The web server, which also has an IDS installed on it, has 4 Gigabytes of Random Access Memory (RAM), 4 Virtual CPUs, and 8 Gigabytes of Hard Drive Space.

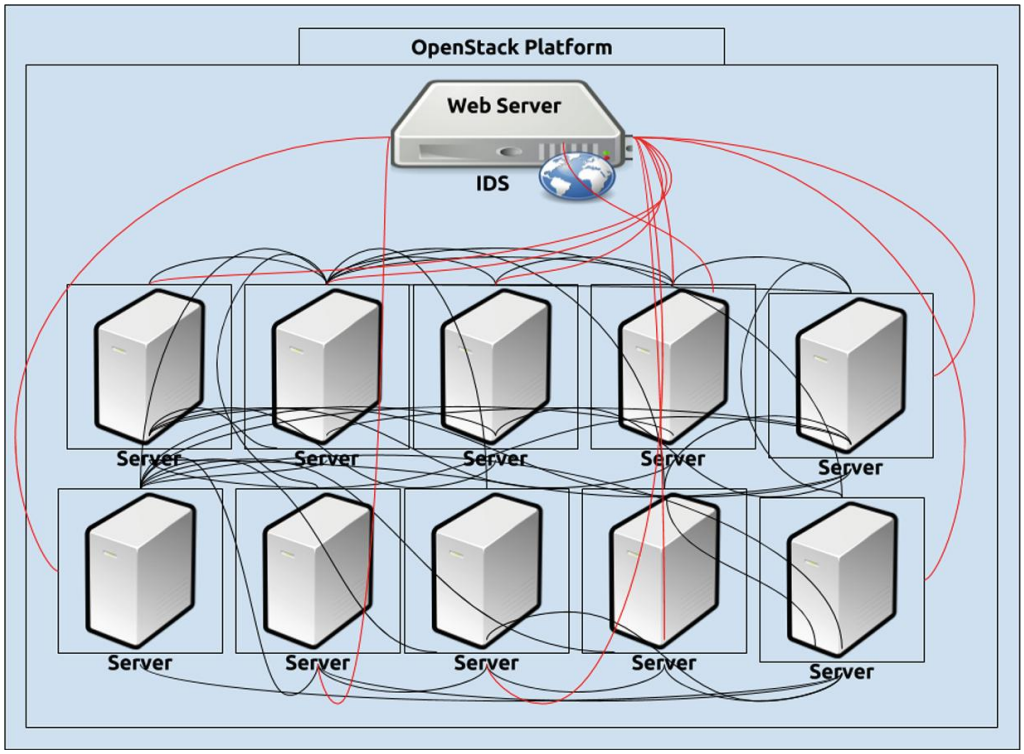

Figure 2: Scenario of the attacks launched during experiments.

When a signature rule was activated, Figure 3 demonstrates that Suricata handled 100 Gb/s worth of garbage. By the contrary, the capacity decreased to 89 Gb/s because 62% of the signs in the setting file had to be utilised of the packets were destroyed. The fact that each instance of Suricata processes each packet by comparing it to one of 300000 possible signatures is the root cause of the high CPU consumption and the high percentage of dropped packets.

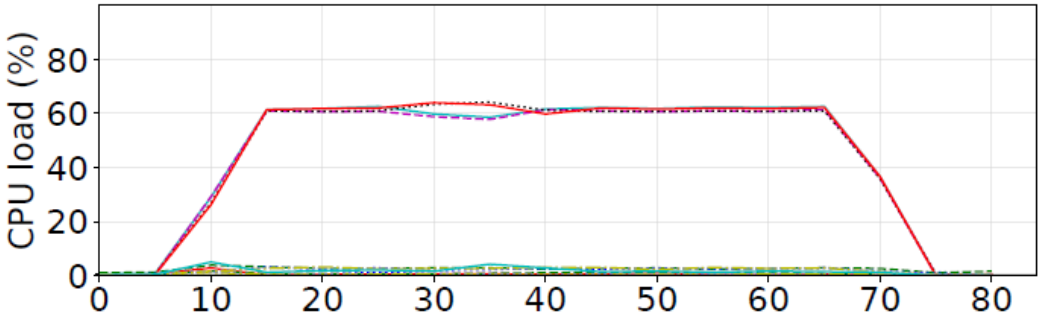

Figure 3: When activating one detector condition retrieved from the Suricata has setup file, measuring the CPU consumption of Suricata and SoftIRQ.

CONCLUSION:

To summarise, the researchers discovered the following after analysing the findings of the experiments that made up this study. This study came to the conclusion that using multi-threading, which is supported by some of the IDSs that were assessed, can assist prevent packet drops, allowing for more efficient processing of network-wide hostile traffic. Suricata's excellent performance in a cloud computing environment was credited to its support for multi-threading and multi-core computers. Within the first five minutes of the DDoS attack's start, the three intrusion detection systems were able to locate it. Further assaults will be tested utilising these three IDSs over an extended length of time in a later part of this research effort. Additionally, different IDS configurations, each with their own set of rules, will be used in this study. It is envisaged that some IDS will be installed and evaluated in IoT scenarios as a result of this study.

REFERENCES:

1) Ugochukwu, C. J., Bennett, E. O., & Harcourt, P. (2019). *An intrusion detection system using machine learning algorithm*. LAP LAMBERT Academic Publishing.

2) Alzahrani, A. O., &Alenazi, M. J. (2021). Designing a network intrusion detection system based on machine learning for software defined networks. *Future Internet*, *13*(5), 111.

3) Li, X. (2018, April). Study on information recommendation of scientific and technological achievements based on user behaviormodeling and big data mining. In *2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)* (pp. 228-232). IEEE.

4) Yan, H., Yu, P., & Long, D. (2019, January). Study on deep unsupervised learning optimization algorithm based on cloud computing. In *2019 international conference on intelligent transportation, Big data & smart city (ICITBS)* (pp. 679-681). IEEE.

5) Wang, Y., Guo, S., Wu, J., & Wang, H. H. (2020, October). Construction of Audit Internal Control System Based on Online Big Data Mining and Decentralized Model. In *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 623-626). IEEE.

6) Hongsong, C., Yongpeng, Z., Yongrui, C., & Bhargava, B. (2021). Security threats and defensive approaches in machine learning system under big data environment. *Wireless Personal Communications*, *117*, 3505-3525.

7) Tchakoucht, T. A., &Ezziyyani, M. (2018). Multilayered Echo-State Machine: A Novel architecture for efficient intrusion detection. IEEE Access, 6, 72458-72468.

8) Rana, P., Batra, I., Malik, A., Imoize, A. L., Kim, Y., Pani, S. K., ... & Rho, S. (2022). Intrusion Detection Systems in Cloud Computing Paradigm: Analysis and Overview. *Complexity*, *2022*.