International Journal of Advanced Research in Engineering and Applied Sciences

ISSN: 2278-6252
Impact Factor: 7.388

A REVIEW AND ANALYSIS OF INTRUSION DETECTION SYSTEMS IN CLOUD COMPUTING SYSTEMS

DR. RAJESH KUMAR
Assistant Professor in Computer Science
Govt College for Girls Sec-14 Gurugram

ABSTRACT:

Intrusion detection systems (IDSs) are a critical component of any cloud computing environment. They help to protect cloud resources from unauthorized access, malicious activity, and data breaches. The pay-per-use model of Internet service delivery offered by the cloud computing paradigm is swiftly gaining favour because it makes it easier to develop, distribute, and use mobile applications. Security is currently a crucial issue that needs to be addressed due to the open and decentralised nature of the cloud. The appeal that hackers have is primarily due to the sheer amount of data available. The task of developing an efficient IDS must be finished right away. The goal of this study was to determine how well intrusion detection systems work at spotting attacks. In order to conduct the experimental research, an OpenStack cloud platform was set up, and an IDS was built to track all network traffic of the installed web server. The findings show that Suricata is more adept than Bro and Snort in identifying malicious packets and dropping less packets than Bro and Snort sequentially when a DDoS attack is underway.

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

INTRODUCTION:

With the increasing popularity of cloud computing, securing cloud infrastructure has become a critical concern for organizations. Intrusion detection systems (IDS) play a vital role in identifying and preventing cybersecurity threats in cloud environments. This literature review aims to analyze the existing research on IDS in cloud computing systems, focusing on their effectiveness, limitations, and potential enhancements. The review explores various IDS techniques, including signature-based, anomaly-based, and hybrid approaches, while considering the unique challenges and requirements specific to cloud computing environments.

In addition to other security measures like deploying firewalls, anti-virus software, and different access control mechanisms, intrusion detection networks (IDS) are security solutions that can make communications and data networks more safe. Since the development of this technology, many IDS strategies have been proposed in the academic community, but the "Common Intrusion Prevention Framework" (CIDF), also known as the "Common Intrusion Identification Framework," is a team of experts that was established by DARPA in 2019 with the primary objective of directing and developing a uniform structure in the information security sector (Ugochukwu et al. 2019; Tchakoucht&Ezziyyani, 2018). This team has produced some important work in this field. included into IETF in 2000, the team proposed a core IDS design based on an examination of four additional types of functional components, and after deciding on the new acronym IDWT (Fig. 1):

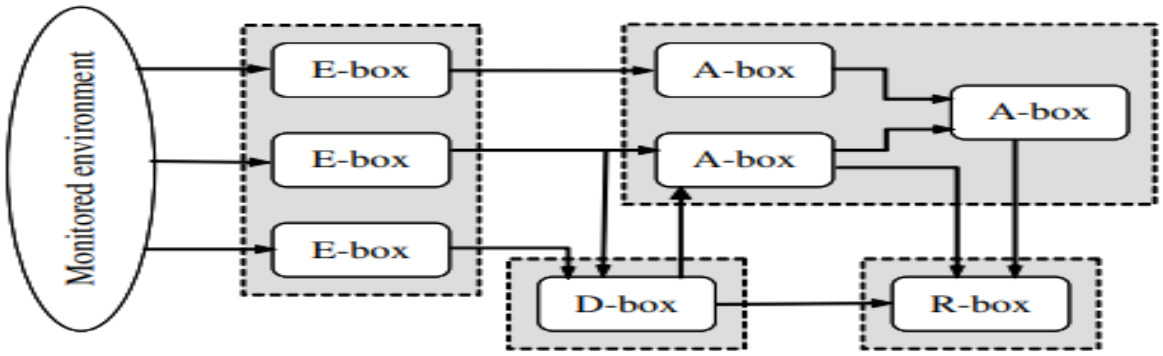

Figure 1: IDS computers' fundamental CIDF configuration (Alzahrani, &Alenazi, 2021)

Intrusion detection systems (IDSs) are a critical component of any cloud computing environment. They help to protect cloud resources from unauthorized access, malicious activity, and data breaches.

In cloud computing environments, IDSs can be deployed in a variety of ways. They can be hosted on-premises, in the cloud, or in a hybrid environment. The deployment method will depend on the specific needs of the organization.

There are a number of challenges to deploying IDSs in cloud computing environments. These challenges include:

- The dynamic nature of cloud environments. Cloud resources are constantly being created, deleted, and moved. This can make it difficult to keep track of all the resources that need to be monitored.
- The large volume of data that needs to be analyzed. Cloud environments generate a lot of data. This can make it difficult for IDSs to keep up with the volume of data and identify suspicious activity.
- The distributed nature of cloud computing. Cloud resources are often spread across multiple locations. This can make it difficult to coordinate the activities of IDSs that are deployed in different locations.

Despite these challenges, IDSs are an essential part of any cloud computing security strategy. They can help to protect cloud resources from a variety of threats, including:

- Unauthorized access
- Malicious activity
- Data breaches
- Denial-of-service attacks
- Malware infections

There are a number of different IDS solutions available for cloud computing environments. These solutions vary in terms of their features, capabilities, and price. When choosing an IDS solution, organizations should consider their specific needs and requirements.

Here are some of the most popular IDS solutions for cloud computing environments:

- Snort is a free and open-source NIDS solution. It is one of the most popular IDS solutions in use today.
- Suricata is a free and open-source NIDS solution that is similar to Snort. It is known for its high performance and scalability.

- OSSEC is a free and open-source HIDS solution. It is designed to monitor individual hosts for signs of intrusion.
- Tripwire is a commercial HIDS solution. It is known for its ease of use and its ability to detect a wide range of intrusions.

These are just a few of the many IDS solutions that are available for cloud computing environments. When choosing an IDS solution, organizations should carefully consider their specific needs and requirements.

Here are some of the best practices for deploying IDSs in cloud computing environments:

- Deploy IDSs in a variety of locations. This will help to ensure that all of the cloud resources are being monitored.
- Use a cloud-based IDS solution. This will make it easier to manage and maintain the IDS.
- Configure the IDS to monitor for a wide range of threats. This will help to protect the cloud environment from a variety of attacks.
- Monitor the IDS logs regularly. This will help to identify any suspicious activity.

By following these best practices, organizations can help to ensure that their cloud computing environments are protected from intrusions.

In cloud computing systems, there are several detection systems in place to ensure the security and integrity of the data and resources. These detection systems include: Intrusion Detection Systems (IDS): IDS detects any unauthorized activities or malicious behavior within the cloud infrastructure. It monitors network traffic, system logs, and user behavior to identify and respond to potential threats. Intrusion Prevention Systems (IPS): IPS is a proactive security measure that detects and blocks any suspicious activity or known vulnerabilities. It helps prevent attacks by blocking malicious traffic and can automatically respond to detected threats. Data Loss Prevention (DLP): DLP systems monitor and prevent the unauthorized transmission or leakage of sensitive data from the cloud. They analyze

data transfers, emails, and other communication channels to enforce security policies and prevent data breaches. Security Information and Event Management (SIEM): SIEM systems collect and analyze security event data from various sources within the cloud environment. They provide real-time monitoring, threat detection, and incident response capabilities by correlating and analyzing logs, alerts, and other security-related information. Anti-malware/Antivirus Systems: These systems protect cloud environments by scanning files and applications for known malware or viruses. They detect and block malicious software to prevent infections and associated risks. Distributed Denial of Service (DDoS) Detection and Mitigation: DDoS detection systems monitor network traffic and detect patterns that indicate a potential DDoS attack. They apply mitigation techniques to protect cloud resources and ensure uninterrupted service availability. Behavioral Analysis Systems: These systems analyze user behavior patterns, application usage, and system logs to detect any abnormal or suspicious activities. They use machine learning algorithms to identify deviations from normal behavior and trigger alerts for potential security incidents. Vulnerability Assessment Systems: These systems scan cloud infrastructure for security vulnerabilities and misconfigurations. They help identify weaknesses that may be exploited by attackers and provide recommendations for remediation.

These detection systems work together to provide a multi-layered security approach, ensuring the protection of cloud computing resources, data, and applications.

literature review

literature review provides a comprehensive overview of cloud computing systems, covering their definition, characteristics, deployment models, service models, benefits, challenges, and adoption trends. It sheds light on the existing body of knowledge and highlights areas that require further research, such as data governance, interoperability, and cloud service integration. Understanding the evolution and adoption of cloud computing systems is vital for individuals and organizations seeking to maximize the potential benefits and effectively navigate the challenges associated with this transformative technology.

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

Namasudra et al., (2020) DNA (Deoxyribonucleic Acid) encryption has been proposed as a new method to improve cloud storage security. In this case, a secret key of 1024 bits was produced to protect the system from various threats. The secret key was generated using user attributes and Media Access Control (MAC) address, DNA bases, ASCII value, and rules like decimal encoding and complementary rule. The theoretical analysis and actual findings demonstrated the superiority of this approach over a number of well-known alternatives.

Aluvalu R and Muddana L, (2015) concerned primarily with safeguarding the privacy of cloud data because of the need of secrecy, trust, and access control in using the cloud. There are several benefits to using distributed computing to make data available to those who cannot be trusted. Successful encryption methods that take into account the granularity of access control are discussed. In addition, many distributed computing control models were investigated.

Arockiam L and Monikandan S, (2014) focuses on methods to provide data access to verified users. The two methods listed above are used to transmit encrypted data throughout the storage management process; ensuring maximum clarity. The goal is to hide the identities of unwelcome customers via the Obstruction process, which is then put into action with the help of either large numbers or sophisticated computer programming. Using an encryption key, encrypted data is converted from a readable to an unreadable format. For encryption, an unreadable format is used. More authentications are provided over questionable data in the cloud thanks to encryption and mucking with systems.

Kavuri S.K.S.V.A et al., (2014) predicted a process in which the customer would choose the specific information needed. Validation key was established by document, which might be media, report, or other evidence. Highly determined message supervising procedure is designed to lessen the risks associated with cloud computing server security. Users' methods of accessing data include spotting uniqueness via message straightness.

Kaur R and Singh R.P, (2014) primarily concerned with ensuring the safety of data storage, this method progresses through three phases: private, public, and hybrid. The three phases

are encrypted at various points to ensure privacy. Two-tier security relies on a unified method of structural organisation. In the public phase, information is encrypted and decrypted, and in the private phase, the token system is put into action. Following the aforementioned procedure strengthens cloud safety and integrity.

Ari Juels and Alina Opera, (2013) projected a framework mainly to maintain high confidentiality to cloud data by maintaining data integrity by continuous verification and reliable data accessibility. The major setbacks are to maintain high security and operational risks like software bugs, malware and hardware failure etc. The more focused task in cloud computing is to secure the outsource data and other setbacks to maintain high data accessibility and reliable assurance.

METHODOLOGY:

The experiments make use of the tools Snort, Suricata, and Bro. All of them are regarded as network intrusion detection systems, or IDS for short. The majority of Snort's users are network administrators, and it has a solid reputation in the business world. The single threaded nature of this program's design is its most annoying feature because it causes a variety of issues and causes many packets to be dropped while Snort is receiving a substantial share of traffic. One may contrast Suricata with Snort. In reality, it is compatible with Snort and can read the log files that are produced by that programme. Suricata, in contrast to Snort, has multi-threading capabilities that enable it to utilise cutting-edge multi-core and multiprocessing technology. This is yet another advantage of the programme.

RESULTS AND DISCUSSIONS:

In order to evaluate the effectiveness of the IDS, the major goal of this investigation was to accurately identify distributed denial supply assaults. This set up 10 workstations, or clients, each running an application written in Python to attack a web server and using the OpenStack cloud computing infrastructure. that was created with this goal in mind. The architecture that was used for this specific assault scenario is described in Fig. 2. Every server runs Ubuntu 14.04 and has four virtual CPUs, two gigabytes of RAM, and four gigabytes of hard drive space. They also individually use the Ubuntu operating system. The web server contains 4 Gigabytes of Random Access Memory (RAM), 4 Virtual CPUs, and 8

Gigabytes of Hard Drive Space. It also has an IDS installed on it.

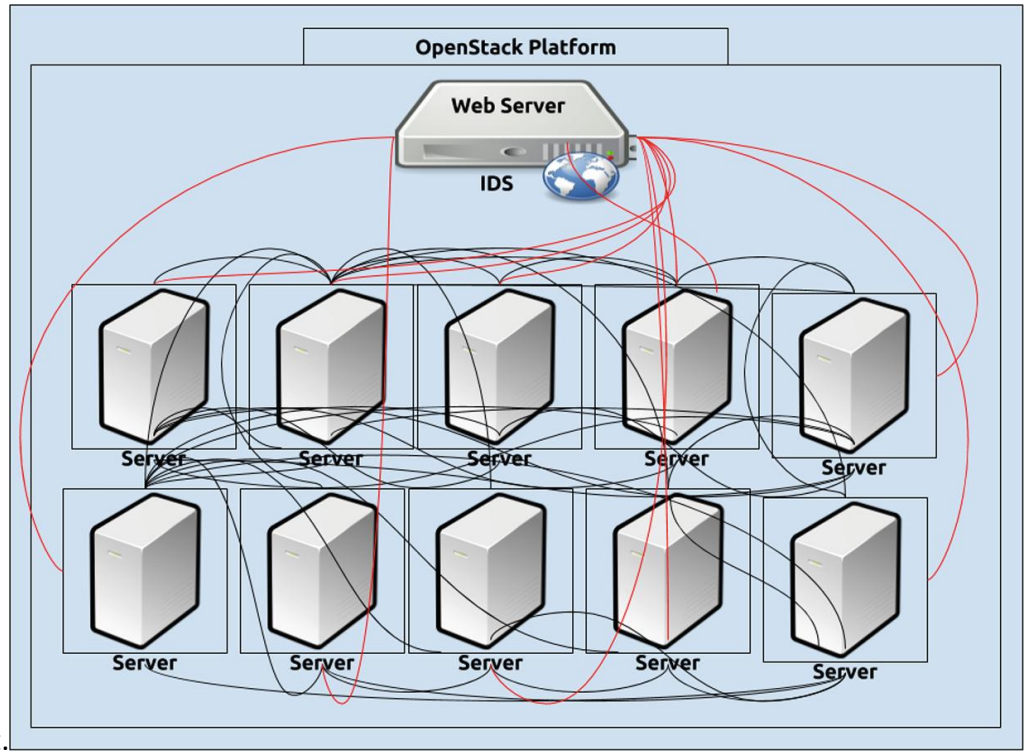

Figure 2: Scenario of the attacks launched during experiments.

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.

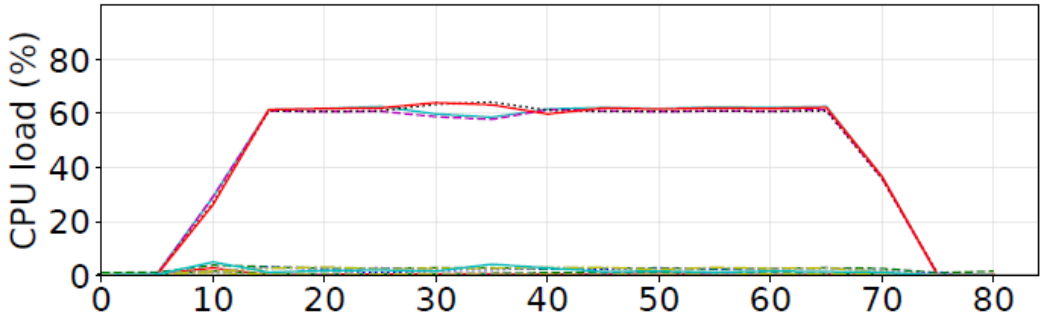

Figure 3: When activating one detector condition retrieved from the Suricata has setup file, measuring the CPU consumption of Suricata and SoftIRQ.

CONCLUSION:

In short, after examining the results of the experiments that made up this study, the researchers found the following. This study found that multi-threading can help avoid packet drops, which enables more effective processing of malicious network traffic. Multi-threading is supported by some of the IDSs that were evaluated. Suricata's support for multi-threading and multi-core machines was praised with contributing to the software's good performance in a cloud computing environment. The three intrusion detection systems were able to find the DDoS attempt within the first five minutes of it beginning. Later on in this study project, more assaults will be tested using these three IDSs for a prolonged period of time. This study will also make use of various IDS settings, each with its own set of rules. As a result of this study, various IDS are expected to be implemented and tested in IoT settings.

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*.

9) Shamir and Y. Weiss, "A New Scheme for Dynamic Broadcast Encryption," Advances in Cryptology—CRYPTO 2021, Springer Berlin Heidelberg, 2021, pp. 1-13.

10) D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," Advances in Cryptology—CRYPTO 2020, Springer Berlin Heidelberg, 2020, pp. 213-229.

11) B. Waters, "Efficient Identity-Based Encryption Without Random Oracles," Advances in Cryptology—EUROCRYPT 2019, Springer Berlin Heidelberg, 2019, pp. 114-127.

12) J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," IEEE Symposium on Security and Privacy, 2017, pp. 321-334.

13) M. Chase, "Multi-Authority Attribute-Based Encryption," Theory of Cryptography Conference, Springer Berlin Heidelberg, 2017, pp. 515-534.

14) D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," Advances in Cryptology—CRYPTO 2004, Springer Berlin Heidelberg, 2019, pp. 41-55.

15) M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Communications, vol. 17, no. 1, pp. 51-58, February 2018.

16) C. Gentry and A. Silverberg, "Hierarchical ID-Based Cryptography," Advances in Cryptology—EUROCRYPT 2022, Springer Berlin Heidelberg, 2022, pp. 548-566.