International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT228110

IDS Based threat monitoring in Cloud Computing

Priya S[1], Dr. R. S. Ponmagal[2]

[1] Department of Computing Technologies, Research Scholar, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India

[2] Department of Computing Technologies, Associate Professor, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India

priyasugam@gmail.com[1], ponmagas@srmist.edu.in[2]

ABSTRACT

Article Info
Volume 8, Issue 1
Page Number : 108-114

Publication Issue :
January-February-2022

Article History
Accepted : 15 Jan 2022
Published : 25 Jan 2022

Cloud computing is one of the most rapidly evolving technologies. Cloud computing has grown in popularity as a result of its benefits such as cost-effectiveness, pay-per-use, scalability, and ease of upgrading. Despite all of these advantages, many firms are hesitant to use cloud environments due to security reasons. The focus of this study is on detecting and identifying theft. It represents a novel way to detecting cyber-attacks in the cloud environment by studying violent attacks patterns using threat assessment techniques. Our solution's goal is to combine information from Intrusion Detection Systems (IDS) implemented in cloud services with risk evaluation data for each attack scenario. Our approach proposes a new qualitative technique for examining each symptom, indication, and risk in order to determine the impact and likelihood of distributed and multi-step attacks against cloud systems. The deployment of this strategy will reduce false positive alarms and improve the IDS' performance.

Keywords - Cloud computing, IDS, Risk Analysis, Security

I. INTRODUCTION

Cloud computing is a new developing concept in information systems that can provide on-demand network access to a shared reservoir of programmable computing resources that can be released with low administration effort and interactions can be delivered quickly. It represents a new potential for both customers and service providers to save IT costs by boosting IT efficiency, agility, and reliability. Cloud systems can automatically control and optimise use to offer an alternative way for trying to rent computing and storage infrastructure services, which enables customers to create an elastic environment. From on-demand allocation and resource grouping similar to rapid elasticity and network access, cloud systems effectively control and optimise resource use to present an alternative way for leasing storage and computing cloud infrastructure. As cloud services are available over the internet, they are vulnerable to a variety of threats that could compromise the reliability, security, and privacy of data stored in the cloud.

Security professionals may find it difficult to detect and deter threats; consequently, the adoption of an IDS (Intrusion Detection System) can assist both cloud providers and security administrators in monitoring and analysing network traffic. The purpose of deploying such a system is to avoid attacks by employing various detection algorithms. Nonetheless, evaluating and monitoring symptoms generates a slew of warnings, the majority of which are erroneous. The proposed correlation approach seeks to assess the risks associated with each attack style. It entails assessing the risk associated with each symptom, indicator, and vulnerability in order to determine the attack risk score, which is then used to generate an alert. It also entails including customers as part of the security protection.

The scope of study is organised as follows: in part II, we review previous research in this topic. The intrusion detection system and threat assessment methodology are presented in Section III, and our proposed detection approach is described in Section IV, which is based on the analysis of attack patterns by risk assessment. The conclusion and future work will be presented in the final section of this paper.

II. RELATED WORKS

Many documents have been created in the previous few years that present IDS and detection methodologies. With the goal of detecting intrusion and reducing false positive alerts, security researchers need a smooth system to integrate and analyse varied information supplied by heterogeneous sources deployed in a cloud environment.

To classify the existence of a threat, the authors of [1] use five main classifiers: categorization by attack vector, classifying by threat objective, characterization by operations and maintenance impact, identification by informational impact, and classification by protection, which provide network administrators with data on how to mitigate or prevent a threat.

S. A. and J. Hamilton [3] developed an ontology-based attack model to analyse the security of an information system from the attacker's perspective, employing approaches similar to those employed in the AVOIDIT [2] taxonomy. The evaluation of attack impacts is the goal of the review process. As a result, the difference between the performance of the system before and after an attacker is calculated. There are four stages to the process. The first approach is to use automated vulnerability tools to detect system flaws. These tools examine a computer system, an application, or a network for risks and generate scan results. The established ontology is employed in the second phase to assess which attacks could occur as a result of the detected risks. The possible impacts are obtained by querying the ontology. Finally, the attack effect is determined in the final stage. The authors of [4] proposed a four-dimensional taxonomy that provides a classification for network and computer assaults. Their taxonomy aids in the improvement of computer and network security, as well as the consistency of language used to describe attacks. The attack is classified using the first dimension, the attack vector. The attack's target is classified in the second dimension. The vulnerability categorization number, or requirements from Howard's taxonomy [5,] is the third dimension. The payload or effects involved are highlighted in the fourth and final dimension. For intrusion detection in cloud computing, Massimo Ficco suggests a hybrid and event correlation approach [6]. It entails gathering a variety of data at various cloud levels in order to do complex event analysis and present the results in an ontology.

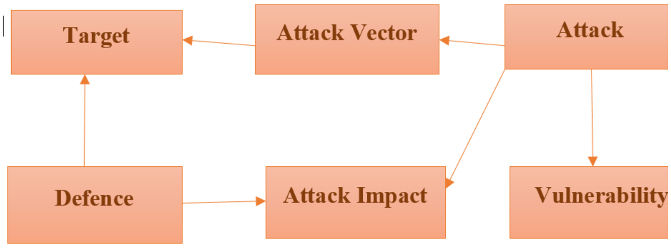

Figure 1 Attack Mechanism

We developed a new intrusion detection approach based on risk assessment in our prior work [7], with the goal of introducing the data owner and cloud provider.

Despite the fact that all of the previous studies give a useful taxonomy and ontology that can provide a meaningful baseline for cyber intrusions and attacks analysis, they lack the details needed to assess all symptoms and attacks, which can result in a large number of false positive alerts. Furthermore, this paper presents a detection method based on risk assessment analysis of the attack pattern, implying that both the data owner and the cloud provider will be included in the attack analysis. The same attack in two distinct services, for example, may have different effects, but it will be identified as malicious in both services.

This could cause IDS to miss the impact analysis, resulting in a slew of false alarms. Our technology specifically tackles this issue by incorporating risk evaluation into the detection process.

Threat Pattern and Risk-Based IDS Analysis

Intrusion detection risk analysis and threat behaviour is presented in this part.

Attack pattern

It is evident to us that a bad user can employ a defined attack pattern to compromise the security in a cloud service using several scenarios of attacks. With the help of the CAPEC (Common Attack Pattern Enumeration and Classification) vocabulary and classification taxonomy, an attack pattern can be defined as the various actions taken by a malicious person to gain access to a system. Figure 1 shows the taxonomy that was used: The pattern is defined by the attack, scenario, indicator, symptoms, and vulnerabilities in this taxonomy.

Each attack has a specific scenario, which is described by indicators and symptoms.

Attack pattern analysis based on risk assessment

Risk is defined as the possibility that a specific threat may launch attacks in an object or collection of assets to produce loss or harm. According to the 27005 specification The chance of successful attacks and the intensity of those attacks, should they occur, are used to assess risk.

Risk = Impact * Likelihood

The amount to which a risk event may influence the company is represented in terms of Confidentiality, Integrity, and Availability, and is referred to as impact (or consequence).

The probability of an event occurring is represented by the term "likelihood." The use of this equation in our methodology encourages customers to estimate the security threats to their data in order to make the analysis of all observed events easier.

In most cases, intrusion signatures are defined as a series of events and conditions leading to a break-in. The context in which the sequencing becomes an intrusion is defined by the requirements. This analysis generates a large number of false alarms and is ineffective in a cloud setting because of the lot of users and Internet accessibility.

The effectiveness of IDS-based risk assessment and attack pattern in identifying real attacks on cloud resources has been demonstrated. This type of IDS analyses and categorises signature attributes in order to extract attack patterns using matching pattern algorithms and a based on behavioral analysis based on a Gaussian method that provides a sharp value for attack risk in order to distinguish between malicious and normal direct requests to a cloud service.

The goal is to redefine the intrusion detection problem as a pattern recognition problem with risk evaluation. Using the proposed Gaussian formula [11], which captures probabilistic correlations among the variables. This method is commonly used in conjunction with statistical schemes for intrusion detection.

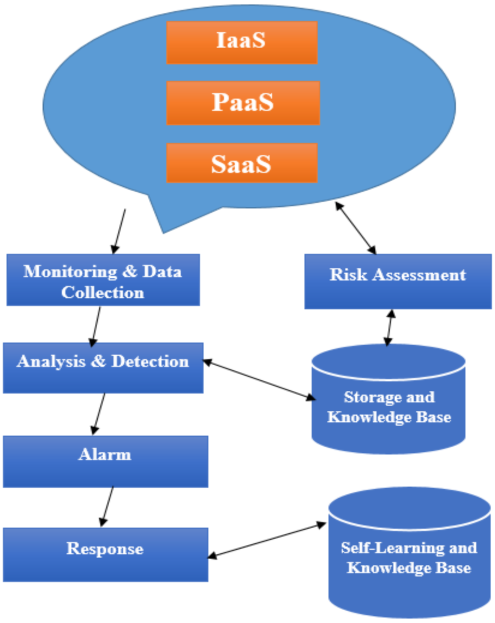
IaaS
PaaS
SaaS
Monitoring & Data Collection
Risk Assessment
Analysis & Detection
Storage and Knowledge Base
Alarm
Response
Self-Learning and Knowledge Base

Figure 2 Risk Analysis Architecture

III. PROPOSED ARCHITECTURE

In this part, we present a scalable intrusion detection system (IDS) architecture based on a software-defined networking environment with vitalization underlying structure. We used OPENSTACK [12] as a cloud platform with a collection of open source software projects that developers and cloud computing technologists can use to build up and run their cloud compute and storage infrastructure in order to achieve our proposed notion. The simulation environment is a multi-layered Cloud environment with a variety of applications and services. Layering and compositions of the proposed intrusion detection solution require that all requests from users to cloud services must transit through the IDS; this case can simplify traffic collecting and analysis.

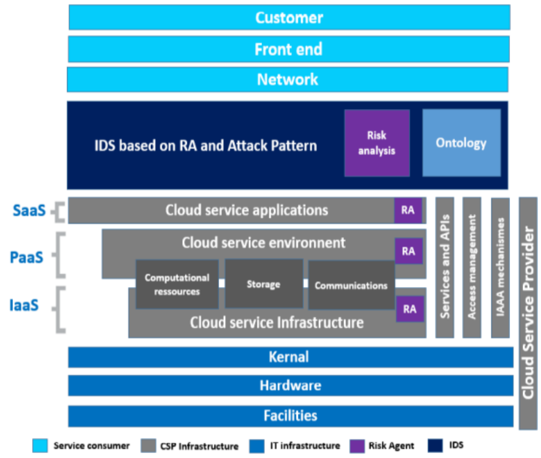

Figure 3 IDS based on cloud Computing

The proposed IDS has three layers

Suricata [12] has been used as an intrusion detection system because it is free and open source. Suricata [12] is a free and open source intrusion detection system that can do real-time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM), and offline pcap processing. For complicated threats identification, robust and broad rules with signature language and scripting capability are used to inspect network data. For complicated threats detection, there are a lot of rules with signature language and scripting capabilities. The risk analyser has been implemented to centralise all risk agents using the formula, which gives the modified value of likelihood and risk associated with a particular pattern. Ontology: The use of ontology aims to provide a detailed analysis of all recognised dangers and symptoms.

A diagram of the proposed architecture, which includes all cloud layers as well as risk evaluation in the intrusion detection system in order to provide a comprehensive image of intrusion detection, the user is included in the proposed architecture as part of the analysis by establishing values in risk agents associated to each attack pattern situation, as shown in the table below. Users become relevant for everyone privacy treatment as a result of this method.

Confidentiality: Only those who are allowed to examine the data in issue should have access.
Data integrity: that unauthorised persons can't change it.

Availability: Ensuring that the cloud service continues to function properly.

Analysis process

In this chapter, we'll go through how our recommended approach was executed in the Cloud, including how service providers and customers were involved in intrusion analysis. The simulation model is a cloud environment with various layers, as shown. We set a fixed figure for the impact of a risk agent deployed in a cloud SaaS for various customers. The major purpose is to evaluate the effectiveness of our job by evaluating all behaviour based on the affects and likelihoods of risks and discovered symptoms.

As shown in Figure 3, our investigation begins with the default SURICAT IDS result, which is a JSON file comprising all alerts. Our investigation began with the formation of connection threes. A SURICATA (Suricata Intrusion Detection System.) events file named log of the data is used as an input in this operation. This log files are typically significant because they provide quantitative aspects of the traffic data (for example, source IP from a collection of network connections, event type). In most cases, these events are saved in the JSON file with the same structure. In the initial step of the study, algorithms are used to build link trees for each connection over a period of time. The goal of this tree is to track all user behaviours while also identifying critical network features that can be used to separate legitimate traffic from malicious activity.

The following stage examines illegal tasks using network trees and attack patterns. In this stage, we leverage the ontology to start creating and using attack patterns. This analytic method will become increasingly relevant as the complexity of threats in the cloud grows. After the pattern has been constructed, we begin an incremental risk analysis based on initial value in the risk agent for each service and client, as well as an evaluation of dependencies between observed events. The result of risk evaluation is able to remove high false alarms as the number of factors involved in attack patterns grows and the quantity of this data grows. If threat risk Rp has an impact on service measured by the customer in the threat agent as the acceptable risks value S, the result of risk evaluation is able to remove false positive alarms. Following the definition of alarm kinds and the use of the generated alerts, the final duty is to update the risk likelihood associated with each occurrence in the risk agent, and then add the received alarms to the IDS's list of known patterns. This method sheds light on the challenge of detecting malicious activity in cloud systems that repeats itself.

IV. RESULT AND DISCUSSION

By involving customers in the protection process and having a thorough understanding of all threat symptoms, signs, and scenarios, it would be easier to detect intrusions and maintain data protection in the cloud. The first findings of implementing intrusion detection risk response and threat pattern with a behavioural analysis technique are shown in this section. Our analysis took into account memory use, CPU usage, and total notification numbers in this trial.

Based on the stated false alarm rate, the efficacy of this strategy has been determined. With these findings, we can see how the false alarm rate has changed over time, and how the analysis-based attack pattern and risk assessment with a probabilistic has decreased false warning rates for known attacks to 0,003%. This method can improve IDS efficiency while also adding security to cloud systems. The graph below depicts the evolution of false alarms as a function of the number of detected alerts before and after the proposed design was implemented.

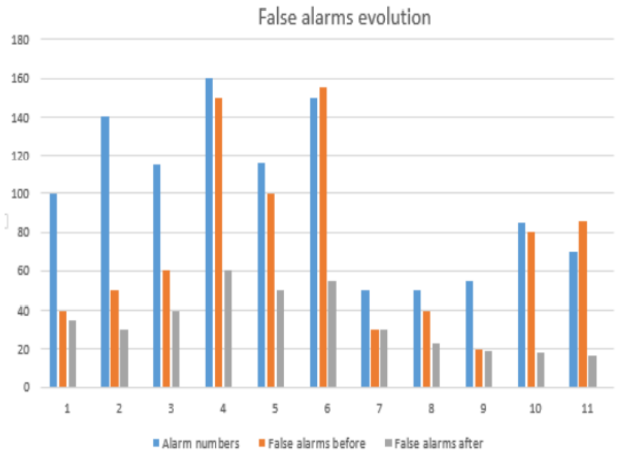

Figure 4. Alerts Evaluation

Time	Number of packets	Number of alarms	Attack Patterns	False Alarm Rate
T1	70000	145	13	4.64%
T2	86000	135	16	4.36%
T3	90000	110	18	3.15%
T4	85000	43	25	0.22%
T5	93000	15	31	0.003%

Table 1 False alarm Rate Analysis

Implementing IDS in a cloud environment based on the proposed architecture with an analysis based on risk assessment and attack pattern demonstrates that the rate of false alarms is less than 0.003% from a known number of attacks and false alerts. This behavioural study can help IDS become more efficient and reduce the number of false alarms.

V. CONCLUSION

One of the most significant challenges that cloud computing services must overcome before they can be widely used is security. The application of risk assessment in intrusion detection can minimise the number of false alerts and boost IDS efficiency, especially in cloud environments, as the preliminary results show. In this research, we present a scalable architecture-based strategy for supporting secure cloud computing for both enterprises and customers. In the same field as intrusion detection systems, we presented a process to be used in intrusion analysis. The process utilizes network virtualization and centralised IDS to provide a comprehensive analysis of all data in cloud networks. For both cloud service providers and clients, the initial results of deployment have proved the efficiency of the suggested architecture and the analytic procedure. Future research will concentrate on combining such an approach with Deep learning algorithms to make the process of analysing and detecting more sophisticated threats easier.

VI. REFERENCES

[1]. D. L. Meena1 and Dr. J. S. Jadon, “Distributed denial of service attacks and their suggested defense remedial approaches,” International Journal of Advance Research in Computer Science and Management Studies, vol. 2 No. 4, April 2019.

[2]. Dr. R. S. Jadon2R. V. Deshmukh and K. K. Devadkar, “Understanding DDoS attack & its effect in cloud environment,” Procedia Computer Science, vol. 49, 2020.

[3]. E. Alomari, S. Manickam, B. B. Gupta, S. Karuppayah, and R. Alfaris, “Botnet-based Distributed Denial of Service (DDoS) attacks on web servers: Classification and art,” International Journal of Computer Applications, vol. 49– No.7, July 2018.

[4]. M. A. Rajab, J. Zarfoss, F. Monrose, and A Terzis, “My botnet is bigger than yours (maybe, better than yours): Why size estimates remain challenging,” Usenix Conference, 2021.

[5]. Incapsula, “Breaking down Mirai: An IoT DDoS botnet analysis,” 2017, https://www.incapsula.com/blog/malware-analysis-mirai-ddosbotnet.html

[6]. S. Gallangher, “Double-dip Internet-of-Things botnet attack felt across the Internet,” 2019, http://arstechnica.com/security/2019/10/double-dipinternet-of-things-botnet-attack-felt-across-the-internet/

[7]. A. Manion, “Security and the Internet of Things,” podcast, 08/25/2019

[8]. Radware Ltd., “DDoS survival handbook”, 2019.

[9]. B. Youssef, M. Nada, B. Elmehdi, R. Boubker, ”Intrusion detection in cloud computing based attack patterns and risk assessment”, Advances in Science, Technology and Engineering Systems Journal, vol. 2, no. 3, pp. 479-484 (2018). [8Youssef, Ben Charhi, et al. ”Intrusion detection in cloud computing based attacks patterns and risk assessment.” Systems of Collaboration (SysCo), International Conference on. IEEE, 2016

[10]. CAPEC, ATTACK PATTERN DEFINITION, 2017.

[11]. ROSADO, Tiago et BERNARDINO, Jorge. An overview of openstack architecture. In : Proceedings of the 18th International Database Engineering and Applications Symposium. ACM, 2014. p. 366-367

[12]. Park, Wonhyung, and Seongjin Ahn.” Performance comparison and detection analysis in Snort and Suricata environment.” Wireless Personal Communications 94.2 (2017): 241-252.

[13]. Suricata Intrusion Detection System., [En ligne]. Available: http://www.openinfosecfoundation.org/index.php/download-suricata.

[14]. P. G. T. e. a. MELL, The NIST definition of cloud computing, 2021

Cite this article as :

Priya S, Dr. R. S. Ponmagal, "IDS Based threat monitoring in Cloud Computing ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 1, pp. 108-114, January-February 2022. Available at doi : https://doi.org/10.32628/CSEIT228110
Journal URL : https://ijsrcseit.com/CSEIT228110