International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Comprehensive Survey of Intrusion Detection System Techniques in Cloud Environment"

Ms. Vijayalaxmi Naganur[1] , Dr. Harish H. Kenchannavar[2]

Submitted:14/03/2024 **Revised**: 29/04/2024 **Accepted**: 06/05/2024

Abstract: The cloud delivers scalable, on-demand virtualized network resources, providing computing infrastructure, applications, and storage services through the internet. Securing the cloud is paramount to shield user data and infrastructure from malicious activities, necessitating the preservation of Confidentiality, Integrity, Availability, and the implementation of timely intrusion detection measures. The integral role of Intrusion Detection Systems (IDS) in monitoring and managing network traffic enhances the security of both user data and cloud services by detecting and preventing fraudulent activities. This study presents a holistic overview of existing security techniques, emphasizing their merits and limitations. It particularly delves into security concerns within each cloud service model, underscores the importance of feature selection and dimensionality reduction, and assesses the current state of IDS technology. IDS techniques are categorized based on their ability to identify attack types, placement, and configurations. Additionally, the study explores strategies like Virtual Machine Introspection (VMI) and Hypervisor Introspection (HVI). The study's structure centers on three main perspectives: cloud security concerns, the significance of feature selection, and a thorough analysis of existing IDS techniques. In conclusion, this work identifies prevalent security challenges and issues, while also highlighting potential areas for future research."

Keywords: *Intrusion Detection Systems, Virtual MachineIntrospection, Hypervisor Introspection*

1. Introduction

Cloud computing offers users versatile services, spanning applications, infrastructure, and storage capabilities, easily accessible and modifiable through the internet. Despite the numerous advantages it offers, cloud computing presents challenges in areas such as security, privacy, load balancing, cost, and performance management. Security, particularly regarding user data and applications within the cloud environment, emerges as a significant concern." Securing cloud computing entails a comprehensive strategy, involving the formulation of policies and procedures to safeguard data, applications, and infrastructure from unauthorized access and various types of attacks. This approach addresses critical issues such as data leaks, tampering, software vulnerabilities, and attacks like SQL injection and flooding. Robust security measures are essential to mitigate risks and ensure integrity, confidentiality, and availability. Numerous security challenges, including a VM escape attack, have been reported by users and providers, emphasizing the need for continuous vigilance in the dynamic landscape of cyber threats. This type of attack highlights vulnerabilities in virtualization environments, where an attacker can break out of a virtual machine and potentially compromise the underlying host system. Such incidents underscore the ongoing need for vigilance and proactive security measures to address emerging threats in the realm of cloud computing. As the technology evolves, it becomes imperative for both subscribers and providers to stay abreast of potential risks and continually enhance security protocols to safeguard sensitive data and infrastructure [2] Security in 2012. In 2013, ENISA [3] reported a distributed denial of service (DDoS) attack on Dropbox, resulting in a complete service outage for 15 days. Symantec disclosed over 450 vulnerabilities [4], including zero-day exploits, in January 2015. Cloud subscribers also encountered a staggering 650 million cyberattacks in 2018."In 2019, cybersecurity faced a surge in IoT attacks, DDoS operations, targeted ransomware, sophisticated phishing, and assaults on containers and cloud services, highlighting the need for robust security measure.

2. Background

2.1 Intrusion detection system (IDS)

Cloud services are commonly classified into three primary types: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Each of these service models introduces specific vulnerabilities and challenges, necessitating tailored security measures [5]. IaaS is susceptible to various attacks, encompassing those targeting virtual machines, virtual networks, hypervisors, DNS, ARP spoofing, cross-site scripting, and data breaches. Implementing effective security measures is crucial to mitigate these risks [6,7,8]. PaaS vulnerabilities include threats such as phishing, Man-in-the-Middle attacks, and port scanning, while SaaS is at risk from Denial-of-Service

[1] *Department of Computer Science and engineering, Jain college of Engineering and Research,,Belagavi-590008, Visvesvaraya Technological University, Belagavi, Karnataka – 590018, India*
ORCID ID : 0009-0008-3648-8040
[2] *Department of Information Science and Engineering KLS,Gogte Institute of Technology,Belagavi-590006, ", Visvesvaraya Technological University, Belagavi, Karnataka – 590018, India*
ORCID ID : 0000-0001-7369-0565

(DoS) and Distributed Denial-of-Service (DDoS) attacks, authentication breaches, and SQL injection attacks. Implementing robust security measures is essential for mitigating these threats [1]. Addressing security risks and countering malicious activities in cloud environments requires the development and implementation of intrusion detection systems (IDS). There are two main types of Intrusion Detection Systems (IDS): host-based IDS (HIDS), which monitors activities on individual hosts, and network-based IDS (NIDS), which analyzes network traffic for signs of malicious activity. HIDS is effective for insider threats, while NIDS is well-suited for detecting network-wide attacks. These systems play a vital role in enhancing cloud security, enabling proactive threat detection. Through the adoption of effective security measures, including intrusion detection systems, cloud service providers can provide users with a more secure computing environment, ensuring the protection of data and applications."

A Host-based Intrusion Detection System (HIDS) monitors individual machines, analyzing the operating system, system calls, files, and applications for internal modifications. It alerts to unusual behavior, primarily used for insider threat detection. In contrast, a Network-based Intrusion Detection System (NIDS) is strategically positioned within networks, monitoring both internal and external traffic. It observes all devices connected to the network, aiming to identify malicious actions or anomalies. Both HIDS and NIDS play crucial roles in enhancing security within cloud environments.[9,10,11]. Each approach offers distinct advantages and constraints. Indeed, a comprehensive cloud security strategy often involves a combination of HIDS and NIDS. HIDS protects individual machines from internal threats, scrutinizing system-level activities. Meanwhile, NIDS monitors network-connected devices, such as firewalls, routers, switches, and print servers, to defend against external attacks. The effectiveness of an Intrusion Detection System (IDS) is contingent on its setup and the methodology used for intrusion detection, underscoring the importance of careful implementation in establishing robust cloud security.

2.2 Feature selection

Feature extraction plays a crucial role in enhancing system accuracy and reducing the false alarm rate (FAR) by addressing challenges related to data dimensionality. The substantial volume, variety, and velocity of network data from multiple devices pose a significant challenge. However, using raw data directly for Intrusion Detection Systems (IDS) can compromise performance. The raw network traffic audit data, with 41 features per packet, results in an impractical number of subsets, straining memory resources and increasing costs. Categorizing network traffic features into irrelevant, weakly relevant, and strongly relevant groups based on their intrusion detection significance is essential. Therefore, preprocessing raw data to eliminate irrelevant features and reduce dimensionality becomes crucial for improving system accuracy.

Feature selection is a method that preserves essential original data attributes. This technique eliminates irrelevant features while retaining those representing the core data. Accurate subset selection is pivotal, as system accuracy relies on intrusion detection features. Researchers have crafted diverse feature selection techniques employing various algorithms. For instance,[12] proposed a Genetic Algorithm (GA)-based approach for feature selection, acknowledging that identifying the right feature set is a challenging and time-consuming endeavor, often requiring domain knowledge expertise. Therefore, an automated feature selection approach is imperative.

Numerous feature selection techniques have emerged in literature, aiming to enhance system performance, trim memory usage, and reduce processing time.[13] Introduced an Intrusion Detection System (IDS) that utilizes feature selection to enhance detection accuracy and efficiency. [15] Put forth an IDS technique using rough set theory to slash feature count to half of the original set. Their work demonstrated that feature selection alleviates system complexity while boosting performance.

a. The primary methods for feature selection encompass the Filter method, Wrapper method, and Embedded method

b. Filter Technique

The most prevalent approach for feature selection involves computing a threshold value to determine the retention or discarding of a feature. This method is directly applied to thedata[12]. It's cost-effective compared to other methods, but its efficacy diminishes when redundancy is low[14] employed the TShark tool to extract valuable features from network traffic forintrusion detection.

c. Wrapper Technique

The wrapper technique functions through three stages: firstly, it calculates feature subsets representing the data. Next, these subsets are categorized and evaluated using an objective function. Finally, an optimal feature subset is chosen to improve system accuracy [12]. Although the wrapper approach tends to outperform the filter method, it requires more computational power and resources. In addressing this, [12] introduced a GA-LR wrapper approach for feature selection in network intrusion detection.

d. Embedded Technique

In the embedded technique, the system learns the optimal feature subset during model creation, making it quicker than both filter and wrapper methods. Embedded methods

primarily use penalization techniques for feature selection, often leveraging the Least Absolute Shrinkage and Selection Operator (LASSO) for regression. These methods have low computational costs and are less susceptible to overfitting. [16] Developed a Network Intrusion Detection System (NIDS) utilizing a feature selection method, specifically employing a binary bat algorithm with two fitness functions. This approach successfully reduced the number of traffic features from 44 to 26, resulting in an enhancement of system accuracy. Likewise,[14] Implemented the Particle Swarm Optimization (PSO) algorithm for feature selection, leading to improved anomaly detection characterized by increased accuracy and reduced False Alarm Rate (FAR). Their study includes a comparative analysis underscoring the importance of feature selection in enhancing intrusion detection systems.

2.3 Dataset for Performance Evaluation

In evaluating Intrusion Detection Systems (IDS), having a representative dataset that mirrors real-world network traffic scenarios is crucial. While researchers have utilized various datasets like KDD99, NSLKDD, and ISC2012, these datasets often lack realism due to missing and redundant records. The presence of redundant records can introduce bias in classifier outputs, favoring repetitions. To address these shortcomings, [20] introduced the UNSW-NB15 dataset in 2015 for more realistic IDS performance evaluation. Network traffic features are categorized into three groups: irrelevant, weakly relevant, and strongly relevant, based on their significance in intrusion detection. Therefore, preprocessing raw data to eliminate irrelevant features and reduce dimensionality is essential for enhancing system accuracy.

To address these limitations, [21] introduced two novel datasets: CICIDS2017 and CSE-CIC-IDS-2018. These datasets capture modern attacks, reflecting current trends, and are constructed based on two networks: the victim network and the attacker network. Encompassing six attack profiles—Brute force, heartbleed, botnet, DoS/DDoS, web attack, and infiltration attack—these datasets were developed in two steps. Initially, 80 flow-based features were extracted from pcap files. Subsequently, the significance of all 80 features was analyzed, and optimal features were determined using a random forest regressor. These selected features were evaluated using machine learning algorithms. To contextualize their work, the authors conducted a comparative analysis against existing datasets.

Over the past decade, substantial research has been dedicated to addressing security and privacy concerns in cloud computing. Upon reviewing the challenges and solutions within cloud security, the importance of intrusion detection systems (IDS) emerged prominently. IDS plays a pivotal role in safeguarding cloud infrastructure, applications, and user data from malicious activities. Thus, the objective of this study is to critically assess existing IDS techniques. The review encompasses the classification and analysis of these techniques, evaluating their strengths and weaknesses, providing an overview of various attack types, emphasizing the importance of feature selection within IDS methods, and examining the availability of datasets. Additionally, the study identifies gaps in current research and outlines future trends to enhance security and privacy measures. The specific goals include conducting a comprehensive analysis of existing IDS techniques, categorizing them into five groups based on intrusion detection type, placement, and configuration: (1) Signature-based IDS, (2) Anomaly detection-based IDS, (3) VM introspection-based IDS,

(4) Hypervisor Introspection-Based IDS, and (5) Hybrid IDS techniques.

Discussing the significance of feature selection as it enhances the accuracy and performance of intrusion detection systems

3. Related surveys

In preparation for our own survey, an extensive review of the existing body of research was conducted. Numerous studies have explored the impacts of attacks and vulnerabilities within cloud computing. For instance, [22] examined the fundamental requisites of cloud security—confidentiality, availability, and integrity. Meanwhile, [23] delved into attacks, vulnerabilities, threats, and security concerns across various cloud computing layers. [24] focused on cloud resiliency, malware, and virtual machine manager (VMM) security. [25] delved into traditional attacks and explored machine learning's potential in managing them, while also providing a threat model for diverse attacks and their remedies. While these surveys dissected issues influencing cloud security, they did not delve into providing solutions.**"**Furthermore,[26] addressed attacks on Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS), providing a comprehensive list of threats in cloud computing. The identified threats included data loss, breaches, malicious insider threats, and account and service hijacking. Additionally, the paper outlined security attacks and proposed potential solutions. [7] outlined eight common factors impacting cloud confidentiality, integrity, and availability. This study examined varying levels of attacks, their surfaces, threats, vulnerabilities, and security requisites in the cloud environment. However, it suffered the same limitation, lacking discussions about specific security techniques to address these cloud computing challenges. On a similar note, [27,28] furnished literature surveys on intrusion

detection systems. However, both articles focused on techniques such as signature-based IDS, anomaly-based IDS, and hybrid methods, without considering VM Introspection (VMI) and Hypervisor Introspection (HVI).”In light of these related surveys, it's evident that several studies have focused on cloud computing security, attacks, intrusion detection, and prevention systems. Despite numerous surveys, there is a notable gap in the exploration of VMI and HVI intrusion detection techniques. A prevailing limitation in the current body of research is the lack of discourse regarding the significance of feature selection and datasets. Feature selection techniques have the potential to augment system performance, accuracy, and overall security cost-effectiveness. Thus, our present study focuses on existing Intrusion Detection System (IDS) techniques, emphasizes the importance of feature reduction, and addresses the pivotal role of datasets.

4. Research methodology

This study's design adheres to the systematic review approach proposed by cited reference papers [29,30]. The core objective of this undertaking is to discern the prevailing landscape of available IDS methodologies, gauging their advantages and limitations. Given the diverse strategies deployed for securing cloud infrastructure, their evaluation necessitates an assessment grounded in a range of security prerequisites. The scope of this paper encompasses a broad array of techniques tailored to furnish security across varying strata of cloud architecture. In our thorough research, we diligently surveyed reputable journals, conferences, and publications covering the period from January 2010 to June 2020 to accumulate insights into cloud security. Our exhaustive inquiry encompassed well-established databases, including Springer, ScienceDirect, Scopus, IEEE Xplore, ACM Digital Library, and Google Scholar. Furthermore, we formulated a set of pertinent keywords to facilitate article retrieval from the aforementioned databases. These keywords were specifically oriented toward addressing security challenges and their cloud-based solutions. Some frequently employed keywords include "security," "intrusion detection”,"intrusion prevention," "feature selection," "dimensionality reduction importance," "attacks," "security challenges," and "datasets" in the context of cloud computing. After scrutinizing abstracts, we judiciously discerned the relevancy of individual articles to our study. Selected publications were subjected to close examination and analysis, thereby enabling us to proffer a comprehensive survey of extant IDS solutions in cloud computing, tailored to combat diverse intrusion scenarios. Figure 1 illustrates the proportion of information sources harnessed for this study.

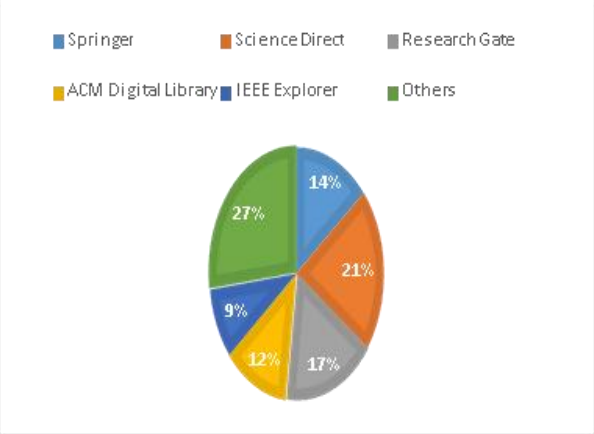

Fig1. Source of Research articles surveyed included in present work

5. Survey of existing ids in cloud computing

This section undertakes the classification and analysis of diverse intrusion detection techniques. Our approach involves categorizing IDS techniques based on their configuration, placement, and their ability to detect specific attack types. The resulting classification encompasses five distinct categories, as follows

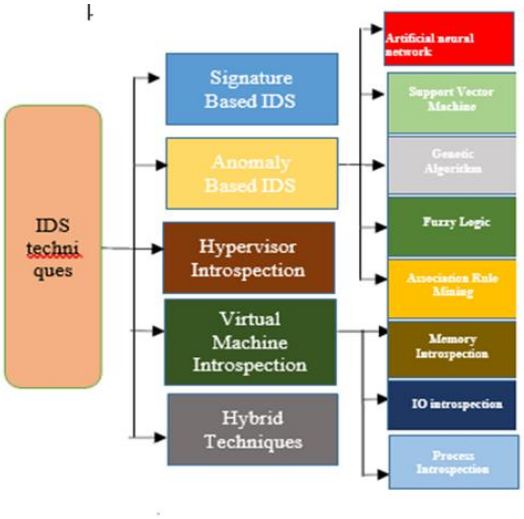

Fig2. Classification of IDS Techniques

5.1 Signature based IDS

Signature-based IDS operates by identifying current suspicious activities through a comparison with established patterns or known malicious instructions. It relies on a signature database, containing records of various attacks and malicious behavior, which requires regular updates to effectively detect recent threats. The method involves matching the present network packets against stored rules to uncover malevolent activities. Snort is a prominent example of this approach, developed by[31], Snort serves as a widely adopted signature-based IDS for real-time network traffic monitoring and packet capturing.

Fig.3 illustrates Snort's essential components, including packet decoder, pre-processor, detection engine, and logging

and alerting system. Incoming traffic undergoes preprocessing to eliminate redundant or incomplete data before being passed to the detection engine. This engine then compares the packet against records stored in the signature database. If a match is found, an alarm is triggered for the relevant authority; otherwise, the packet is treated as normal[31]. Various researchers have explored signature-based approaches in Intrusion Detection Systems (IDS). For instance, in their work, [32] introduced a Network-based Intrusion Detection System (NIDS) relying on rules to identify known attacks within a cloud environment. This system establishes detection rules by dynamically collecting and updating information from the operating system of each virtual machine.(VM).Additionally,[33]proposed a cooperative intrusion detection framework (CGA)in which each server's IDS comprises a combination of a signature database and a block. Table, recording recent attacks. The block table is checked before signature matching, prioritizing recentattack likelihood[34]developed signature-based IDS techniques that leverage a mismatch policy to identify attacks, based on the higher probability of a mismatch in malicious network traffic situations.[35] The proposed IDS technique is signature-based, specifically designed for application-level attacks. The approach entails placing a sniffer between the cloud provider and the user to capture packets for parsing. A parsing grammar is then employed to analyze the parser output against stored semantic rules, generating results accordingly. This approach was detailed in their 2016 study, [36] introduced a Network Intrusion Detection System (NIDS) that employed the SNORT framework for use in OpenStack cloud environments.Their NIDS was specifically designed to categorizevarious types of network attacks. Their research concluded that within OpenStack cloud setups, User Datagram Protocol(UDP) floods could potentially lead to Denial of Service (DoS) attacks. To assess its effectiveness, the authors conducted performance evaluations on an OpenStack privatecloud. In a separate study published in 2017,[37]introduced asignature-based Intrusion Detection System (IDS) incorporating the Myer algorithm. To enhance efficiency in signature matching, they harnessed the power of theMapReduce framework. Furthermore, the authors utilized a multi-core CPU to parallelize the signature matching process,leading to a notable reduction in execution time and memoryusage.

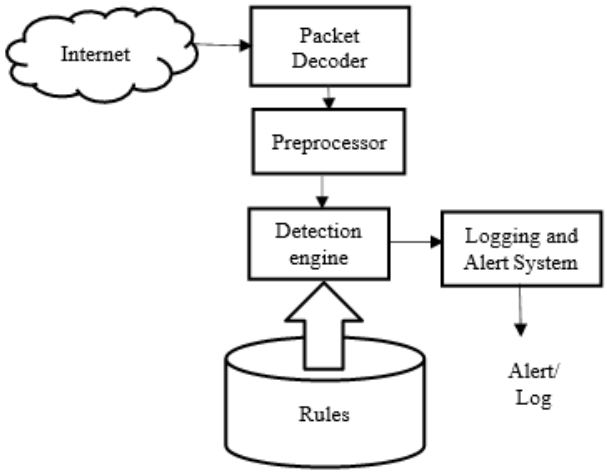

Fig3. Signature Based IDS

5.2 Anomaly-detection-based IDS

In swiftly identifying known attacks with minimal false positives, signature-based Intrusion Detection Systems (IDS) exhibit proficiency, albeit necessitating regular updates to their signature databases. Acknowledging the limitations intrinsic to signature-based IDS, anomaly detection techniques have gained prominence. This methodology entails a thorough examination of user behavior to construct a behavioral profile, subsequently utilized for the identification of both known and unknown attacks. Figure 4 illustrates the fundamental operational model of an anomaly detection technique, encompassing two crucial phases: the training phase and the detection phase.

During the training phase, the feature construction module gathers data from host machines or networks and conducts preprocessing to generate relevant features.

In the training modules, these features are utilized to create a behavioral model that categorizes data as either normal or abnormal, indicating intrusion. In the anomaly detection phase, this model is applied to identify any deviations from normal traffic, subsequently triggering an alert to the security administrator.[38].

While anomaly-based techniques can detect novel attacks, they demand substantial computational resources, and the interpretation of alarms resulting from deviations falls to the security manager. Anomaly-based techniques are categorized based on the methods used for anomaly detection, such as Machine Learning, Fuzzy Logic, Support Vector Machine, and Data Mining. In recent years, several studies have explored these techniques.

For instance, [39] employed a hidden Markov technique utilizing system call frequencies from log files to detect malicious activities.

This technique resulted in the development of three profiles (low, middle, and high) based on recent activity features, each matched using predetermined threshold values.

[40] The proposed approach involves using machine-learning techniques based on the static analysis of program behavior. The method operates in two phases: decoding programs and creating context-free grammars to represent the process flow.[41]introduced an IDS technique combining unsupervised learning and supervised classification, while [42] used normal/abnormal system call frequencies for intrusion detection.[43] One study introduced an entropy-based IDS designed for identifying unknown attacks in cloud environments. Additionally, Gupta & Kumar (2015) developed a system call-based anomaly detection method specifically focused on low-frequency attacks. [44]utilized the support vector machine (SVM) for anomaly detection, and [45] Another approach involved creating an IDS based on artificial neural networks (ANN) for detecting intrusions at various nodes.

While these techniques primarily address traffic attacks such as DoS/DDoS and IP spoofing, it's important to note that they may not comprehensively cover threats like worms, viruses, and rootkits. [46]combined fuzzy C-means and ANN to reduce false alarms and enhance system accuracy by grouping the large database into clusters for training various ANN modules.

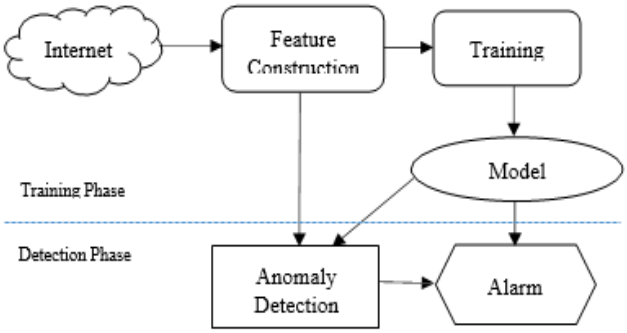

Fig4. Anomaly Based IDS

5.3 Virtual machine introspection (VMI)-based IDS

The positioning of an Intrusion Detection System (IDS) plays a critical role in the intrusion detection process. When an IDS is situated on the host, it enjoys complete visibility of the system but is vulnerable to attacks. Conversely, if an IDS is placed within a cloud network, it becomes less susceptible to attacks, but system visibility is limited. Similarly, conducting analysis on the tenant The use of Virtual Machines (VMs) introduces the risk of the analysis component being compromised by sophisticated malware programs, potentially facilitating intruders in breaching the monitored VM's security. To address this concern, a technique known as Virtual Machine Introspection (VMI) is employed. In VMI, VMs are monitored from an external perspective by collecting data at the hypervisor level. This approach aims to isolate the Intrusion Detection System (IDS) from the monitored VM, and it involves deploying a security tool within the Virtual Machine Manager (VMM) [47] A rudimentary representation of the Virtual Machine Introspection (VMI) technique is depicted in Figure 5. In this model, the monitoring VM acquires state information from the monitored VM through the utilization of the LibVMI library. Serving as a foundational element of the VMI technique, the LibVMI library facilitates the interpretation of information within VMs by processing raw data [48]. Researchers employ diverse methods to gather data from the monitored VM, incorporating memory introspection, system events or process introspection, and Input/Output (I/O) introspection. Approaches based on memory introspection involve the extraction of data from the main memory, while I/O introspection encompasses interactions with hardware. This encompasses file system call introspection, interrupt request introspection, and system call introspection(a service request to the kernel)[49].

[50] “A system was created through kernel debugging to monitor the kernel file system, employing LibVMI for direct memory access [51]. This system meticulously examined system calls and actively opened known backdoor ports to identify potential malicious activities [48]. A two-phase Virtual Machine Introspection (VMI)-based approach was introduced to oversee user in-VM activity. In the initial phase, the authors utilized system calls to generate training data, and subsequently, these feature vectors were applied for classification during the detection phase [52]. The Nitro VMI framework, a Python-based tool, was introduced as a framework for application development that utilizes Nitro web to monitor Virtual Machines (VMs) for intrusion detection. It's essential to acknowledge that this assumption may be compromised by insiders in a cloud environment [53]. The proposal encompassed a Virtual Machine Introspection (VMI) technique specifically tailored for detecting rootkit attacks and malware. This approach involves accessing CPU registers and memory to obtain low-level information crucial for intrusion detection.

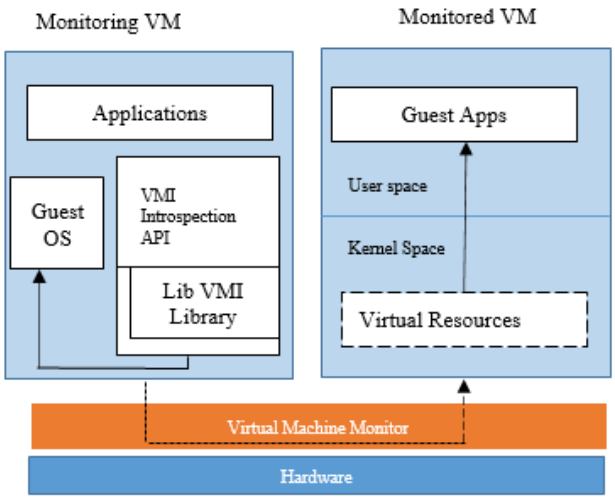

Fig5. Virtual Machine Introspection

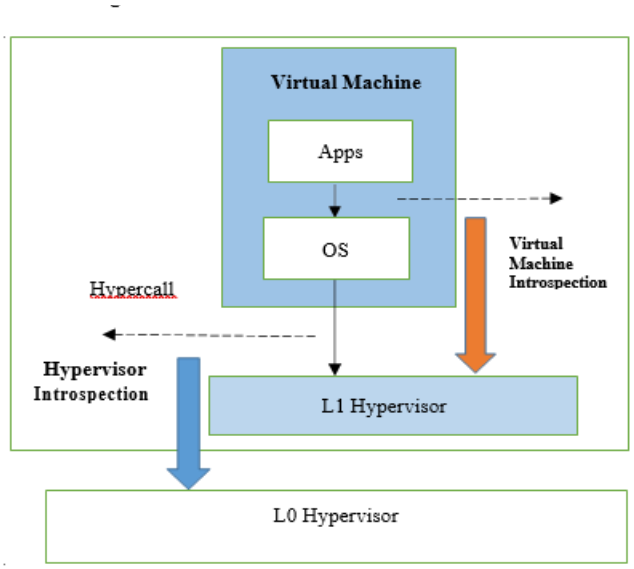

Fig6. Hypervisor Introspection

5.4 Hypervisor-introspection (HVI)-based IDS

Traditionally, Virtual Machine Introspection (VMI) techniques operate under the assumption that the hypervisor provides a secure environment for deploying VMI tools. However, a 2014 report from the National Institute of Standards and Technology (NIST) pointed out vulnerabilities in hypervisors like Xen and VMware ESX that could be exploited by attackers. A compromised hypervisor opens the possibility for launching attacks on Virtual Machines (VMs).

To address these concerns, a novel technique called Hypervisor Introspection (HVI) has emerged. Unlike Virtual Machine Introspection (VMI), HVI does not deploy security tools at the hypervisor level; instead, it operates below the hypervisor. It scrutinizes control and non-control flow data, memory, hypercalls, and hypervisor-related data structures. This approach has garnered attention in intrusion detection research, with researchers exploring its potential capabilities.

For instance, [54] The proposal involves a nested virtualization-based security approach where a security model is placed beneath the Virtual Machine Monitor (VMM). This approach relies on the assumption that if the VMM is compromised, it won't impact the data of guest VM. Similarly, [55] introduced the HyperLock technique, which employs a separate address space to execute the hypervisor. According to this research, the safety of other virtual machines in a cloud environment ismaintained even in the event of a compromise of the hypervisor by an attacker. An advantage of Hyper-Verify is its system flexibility as it does not rely on specific hardware components, allowing for ongoing improvements to an Intrusion Detection System (IDS) even after its deployment. [56] introduced a system capable of analyzing running programs in Virtual Machines (VMs) through the use of VMM (Virtual Machine Monitor) Introspection, as illustrated in Figure 6

5.5 Hybrid Techniques

A single IDS technique may not be comprehensive enough to detect all types of attacks in a cloud environment. To address this, a combination of different IDS techniques is often employed, creating a more robust defense network known as a hybrid intrusion detection system (IDS). Many researchers have presented various combinations of IDS techniques for intrusion detection in cloud environments. For example,[58] introduced a hierarchical architecture featuring multiple security components to provide security as a service. [44] combined Snort with Support Vector Machine (SVM) for anomaly detection. Singh et al. (2016) employed a combination of the decision tree classifier and SVM for anomaly detection, along with Snort for known attacks. [58] The employed approach utilized two algorithms: the packet scrutinization algorithm and the clustering algorithm K-means, in conjunction with artificial neural networks (ANN) to analyze network traffic. [59] The approach utilized Snort to detect known attacks and various classifiers such as Naive Bayes, Decision Tree, Random Forest, and Linear Discriminant Analysis for anomaly detection.” In Patil's 2018 study, Snort was employed for identifying known attacks, followed by the extraction of packet features. These features were then used for classification with the assistance of three distinct algorithms: Decision tree, Random Forest Classifier, and OneR. Building upon this work, [16] introduced a novel approach known as the hybrid HLDNS method. This method was integrated into the Control VM (CVM) of each physical server, enabling the monitoring of virtual network traffic and external network traffic. When a new virtual machine (VM) was introduced, the framework-initiated network traffic capture using the Libcap library. Subsequently, known attacks were detected through the utilization of Snort. The packets were classified as normal or abnormal, leveraging a Random Forest Classifier. Alerts

were generated based on the information collected from Snort and anomaly detection. Additionally, feature selection was optimized using the binary bat algorithm.[60] "The suggested approach presents a hybrid security model that integrates Snort with Genetic Algorithm (GA) to fortify the Availability, Confidentiality, and Integrity of cloud resources and services. This includes refining Snort rules for detecting Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, coupled with utilizing GA for enhanced anomaly detection."

6. Conclusion and future scope

In this comprehensive study, a spectrum of security concerns and potential malicious activities inherent in different service models within cloud computing has been thoroughly addressed. These issues, ranging from data breaches to disruptive flooding attacks (DoS/DDoS), underscore the critical importance of safeguarding cloud-based data, applications, and infrastructure against unauthorized access. Achieving this goal requires the development and implementation of robust security policies and procedures, ensuring the principles of Confidentiality, Integrity, Availability, and timely intrusion detection within the cloud environment. To conclude our study, we have pinpointed several open issues that merit further exploration in future research endeavors. Despite the abundance of IDS techniques in the literature, the dynamic nature of malicious activities highlights the necessity for continuous enhancements. Therefore, future research should prioritize the integration of diverse intrusion detection techniques while emphasizing feature selection and optimization methods to elevate system performance and enhance detection accuracy.In addition, we have contemplated various strategies for improving cloud security while maintaining cost- effectiveness, underlining the importance of these aspects for future research initiatives.

References

[1] M. Khalil et al., "Cloud computing security: A survey," Computers,vol. 3,no. 1,pp.1-35, 2014.doi:10.3390/ computers 3010001

[2] M. Mimiso,Virtual Machine Escape Exploit Targets xen,2012

[3] L. Marinos,"ENISA threat Landscape 2013," Overview Curr. Emerg. Cyber-Threats, 2013, doi:10.2788/14231.

[4] Symantec Intelligence Report.Available at:https://www. symantec.com/.../intelligence-report-06-2015.en-us.pdf.

[5] Khraisat et al.,"Survey of intrusion detection systems: Techniques, datasets and challenges," Cyber security, vol. 2, no. 1, 2019. doi:10.1186/s42400-019-0038-7.

[6] Aldribi, A.Traore et al., "Computers & security hypervisor based cloud intrusion detection through online multivariate statisticalchangetrack-ing,"vol.88,2020 doi:10.1016/j.cose.2019.101646.

[7] J.P.A. Jebamalar et al,Mining Classification Algorithms: A Comparative Study. Singapore: Springer.10.1007/978-981-13-1882-5,1882.

[8] Prabadevi, B. Jeyanthi et al., "An analysis of security so-lutions for ARP poisoning attacks and its effects on medical computing," Int. J. Syst. Assur. Eng. Manag, vol. 11, no. 1, 1-14, 2020.doi:10.1007/s13198-019-00919-1..

[9] Deshpande, P. Sharma et al.,"HIDS, A host based intrusion detection system for cloud computing environment,"2014. doi:10.1007/s13198-014-0277-7.

[10] S.A. Hofmeyr et al., "Intrusion detection using sequences of system calls," J. Comput. Sec., vol. 6, no. 3, pp. 151-180, 1998. doi:10.3233/JCS-980109.

[11] D. Singh et al., "Collaborative IDS framework for cloud," Int. J. Netw., vol. 18, pp. 699-709, 2016.

[12] C. Khammassi and S. Krichen, "A GA-LR wrapper approach for feature selection in network intrusion detection,"Computers & Security, vol. 70, pp. 255-277, 2017.

[13] Z. Zhang et al., "A many objective-based feature selection model for anomaly detection in cloud environment," IEEE Access Pract. Innov. Open Solut.,vol. 8, pp.60218-60231,2020.doi:10.1109/ACCESS.2020.2981373.doi:10.1016/j.cose.2017.06.005.

[14] A. Rawashdeh,et al., Kasassbeh, M,"An Anomaly-BasedApproach for DDoS Attack Detection in Cloud Environment",Adnan Rawashdeh, Mouhammd Alkasassbeh and Muna Alhawawreh, 2018. doi:10.1504/IJCAT.2018.09353.

[15] M. Prasad et al., urn a, "An efficient feature selection-based Bayesian and Rough set approach for intrusion detection." Appl.SoftComput.J.,vol.87,p.105980,2019. doi:10.1016/j.asoc.2019.105980.

[16] R. Patil et al., "Designing an efficient security framework for detecting intrusions in virtual network of cloud computing," Comput. Sec.,vol. 85, pp.402-422,2019. doi:10.1016/j.cose.2019.05.016.

[17] "Citation, E," S,"A Review of KDD99 Dataset Usage in Intrusion Detection and Machine Learning Between 2010 and 2015,", pp. 0-21, 2016.

[18] M. Subhy and D. Basheer, A Comparison Study for Intrusion Database (KDD99, NSLKDD) Based on Self Organization Map(SOM) Artificial Neural Network, 2018.

[19] S. M. Thampi et al., Lecture Notes in Networks and

Systems125 Applied Soft Computing and Communication Networks, 2019.

[20] N.Moustafa and J. Slay, "'UNSWNB15A comprehensive data set for network intrusion detection systems', 10.1109," MilCIS, p. 2015.73489, 2015.

[21] I. Sharafaldin et al., "Toward generating a new intrusion detection dataset and intrusion traffic characterization"in Proc. ICISSP 2018 – International conference on information systems security and privacy, vol. 2018, 2018-janua, pp. 108-116. doi:10.5220/0006639801080116

[22] M. Zhou et al., "Security and privacy in cloud computing, A survey" in Proc. 6th International Conference on Semantic Computing Knowledge Grid,SKG,vol.10,2010pp.105-112. doi:10.1109/SKG.2010.19

[23] C. Modi et al., "A Survey of intrusion detection techniques in Cloud. Netw.Comput. Appl., vol. 36, no. 1,pp.42-57,2013. doi: 10.1016/j.jnca.2012.05. 003..

[24] R. Denz and S. Taylor, "A survey on securing the virtualcloud," J. Cloud Comput. Adv. Syst. Appl., vol. 2, no. 1,pp. 1-9, 2013. doi:10.1186/2192-113X-2-17.

[25] N. Pandeeswari and G. Kumar, "Anomaly detection system in cloud environment using fuzzy clustering-based ANN,", 2015. doi:10.1007/s11036- 015-0644-x.

[26] L.Alhenaki et al," A survey on the security of cloud computing" in Proc. 2nd International Conference on Computer Applications and Information Security ICCAIS 2019, pp. 1-7. doi:10.1109/CAIS.2019.876949.

[27] K. Arjunan and C.N.Modi, "An enhanced intrusion detection framework for securing network layer of cloudcomputing" in Proc. ISEA Conference on Asia-Pacific Security,ISEASP,2017,110.doi:10.1109/ISEASP.2017.7976988

[28] N.A. Azeez et al., "Intrusion Detection and Prevention Systems: An Updated Review." Adv. Intell. Syst. Comput., vol. 1042, pp.685-696, 2020.doi:10.1007/978-981-329949-8_48.

[29] B. Kitchenham et al., "Systematic literature reviews in software engineering-A systematic literature review," Inf. Softw. Technol., vol. 51, no. 1,pp.7-15, 2009. doi:10.1016/j.infsof.2008.09.009.

[30] Y. Charband and N. J. Navimipour, "Online knowledge sharing mechanisms: 'A systematic review of the state- of-the-art literature and reommendations for future ,2016.doi:10.1007/s10796-016-9628-z.

[31] M. Roesch, 'Snort – lightweight intrusion detection for networks', 229. Available at: http://www.usenix.org, vol. 238, 2015.

[32] C.H. Lin et al.,"Efficient and effective NIDS for cloud virtualizationenvironment"inProc.4thIEEE InternationalConferenceonCloudComputingTechnology,2012,pp.249-254. doi:10.1109/CloudCom.2012.6427583

[33] C. C. Lo et al., "A cooperative intrusion detection systemframework for cloud computing net-works" in Proc.International Conference on Parallel Processing Work, 2010, pp. 280-284. doi:10.1109/ICPPW.2010.46.

[34] Y. Meng et al., "Design of cloud-based parallel exclusive signature matching model in Intrusion detection" in Proc.IEEE High Performance Computingand Communications.

[35] HPCC 2013 IEEE International conference Embed. Ubiquitous Comput.EUC, vol. 2013, 2014, pp. 175-182.doi:10.1109/HPCC.and.EUC.2013.34.

[36] J. K. Mandal et al., "Information systems design and intelligent applications," Proc. Second International Conference India, Adv. Intell. Syst. Comput..,339, vol. 1, pp. 2250-2257, 2015. doi:10.1007/978-81-322.

[37] B. I. Santoso et al., 2016, "Designing network intrusion and detection system using signature-based method for protecting open stack private cloud. Sar i, A." (2015), AReview of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications, pp. 142-154.

[38] M. Aldwairi, "Pattern matching of signature-based IDS using Myers algorithm under MapReduce framework,", 2017. doi:10.1186/s13635-017- 0062-7.

[39] A. Sari,"A review of anomaly detection systems in cloudnetworks and survey of cloud security measures in cloudstorage applications,", JIS, vol. 06, no. 2, pp. 142-154, 2015. doi:10.4236/jis.2015.62015.

[40] P. Kumar et al., "A novel approach for security in cloud computing using hidden Markov model and clustering"in Proc. World Congress on Information TechnologyWICT2011,2011,pp.810-815. doi:10.1109/WICT.2011.6141351.

[41] D. Yuxin et al., "Feature representation and selection in malicious code detection methods based on static system calls," Comput.Sec.,vol.30,no.6-7,pp.514-524,2011.doi:10.1016/j.cose.2011.05.007.

[42] M. K. Srinivasan et al.,"State-of-the-art cloud computing security taxonomies-A classification of security challenges in the present cloud computing environment,"ACM Int. Conf. Proceeding S., pp. 470-476, 2012. doi:10.1145/2345396.2345474.

[43] S.D.Wolthusen,"Detecting anomalies in IaaS environments through virtual machine host system call analysis". In Proceedings of the international journal of internet technology and secured, Translator London, (pp.211-218), 2012.

[44] A. SyedNavaz et al., "Entropy based anomaly detection system to prevent DDoS attacks in cloud," Int. J. Comput. Appl., vol. 62, pp. 42-47, 2013. doi:10.5120/10160-5084

[45] Z.AlHaddadet al., A Collaborative Network IntrusionDetection System (C-NIDS) in Cloud Computing, vol. 8,2016.

[46] J.PachecoandV.H.Benitez,"Filix-Herran,L.C.,& Satam,P,"IEEE Access Pract. Innov.OpenSolut., vols. 1-1, 2020.Artificial neural networks based intrusion detection system for internet of things fog nodes. doi:10.1109/access.2020.2988055.

[47] N. Pandeeswari and G. Kumar, "Anomaly detection system in cloud environment using fuzzy clustering-based ANN,", Mobile Netw. Appl., vol. 21, no. 3, 494-505, 2016. doi:10.1007/s11036-015-0644-x.

[48] J. Pfoh et al., A Formal Model for Virtu-al Machine In- trospection, 2009. doi:10.1145/1655148.1655150.

[49] B. Borisaniya and D. Patel, "Towards virtual machine introspection based security framework for cloud," Sadhana, vol. 44, pp. 1-15, 2019. doi:10.1007/s12046-018-1016-6.2013.

[50] T. K. Lengyel et al., "Scalability, fidelity and stealth inthe DRAKVUF dynamic malware analysis sys-tem" in Proc. ACM Internation-al Conference ProceedingSeries.2014-Decem,2014,pp.386-395.doi:10.1145/266424 .2664252.

[51] A.K.M. Virtual machine introspection based spurious process detection in virtualized cloud computing environment, 2016.

[52] S. Lauren and V. Leppanen, Virtual Ma-chine Introspection Based Cloud Monitoring Platform, 2018,pp.104-109. doi:10.1145/3274005.3274030

[53] P. Mishra et al.,"vProVal, Introspection based process validation for detecting malware in KVM- based cloud environment" in Proc. 4th International Conference on FOG and Mobile Edge Computing, 2019,pp. 271-277. doi:10.1109/FMEC.2019.8795365.

[54] Y. Zhang et al., "Cross-VM side channels and their use to extract private keys" in Proc. ACM Conference on Computer and Communications Security, 2012, pp.305-316. doi:10.1145/2382196.2382230.

[55] Z. Wang et al., "Isolating commodity hosted hypervisors with hyperlock" in Proc. EuroSys 2012 Conference, 2012, pp. 127-140. doi:10.1145/2168836.2168850.

[56] J. Shi et al., "Hardware assisted hypervisor introspection," Springer Plus,vol. 5, 647, 2016. doi:10.1186/s40064-016-2257-7.

[57] M.Ficco et al.,"Intrusion detection in federated clouds, "Int. J. Comp. Sci. Eng.,vol. 13,no. 3,pp.219-232, 2016. doi:10.1504/IJCSE.2016.078929.

[58] V. Balamurugan and R. Saravanan, "Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation," Clust. Comput., vol. 22, no. S6, pp. 13027-13039, 2019. doi:10.1007/s10586-017-1187-7

[59] K. Arjunan and C.N. Modi, "An enhanced intrusion detection framework for securing network layer of cloudcomputing" in Proc. ISEA Conference on Asia-Pacific Security,ISEASP,2017,1-10. doi:10.1109/ISEASP.2017.7976988.

[60] T.Ahram et al., "1131 intelligent human systems integration," Adv. Intell. Syst. Comput., vol. 2020, 2020.