



Intrusion Detection System for Cloud Computing

Aditi Laxmi Giri*, S. Annamalai**

*PG Scholar, School of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India

** Associate Professor, School of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India

aditi3699@gmail.com, s.annamalai@galgotiasuniversity.edu.in

1811

Abstract— Cloud computing seems to have become the favoured choice of every IT firm since it offers a flexible and pay-as-you-go services model to its consumers. Even after numerous advancements in cloud technology making. Despite the fact that cloud computing is the most widely used technology today, it still faces several challenges related to security which restricts users from using cloud services for confidential data. The main reason for such security issues in the cloud environment is its open and dispersed nature which makes it vulnerable to a variety of threats and attacks. To get users to consume cloud services, trust must be earned, which can only be done if the infrastructure is well safeguarded, because breaches or cyberattacks at this level jeopardize the entire system. The cloud system becomes quite vulnerable to any kind of intrusion attack attempts like Cross-Site Scripting (XSS) and Distributed Denial of Services (DDOS) because of its distributed structure. Providing security in a distributed system such as the cloud environment necessitates more than just some user authentication via passwords or digital certificates and data transfer secrecy.

The most popular approach for detecting cloud threats is the intrusion detection system (IDS). This paper aims to give an overview of the various cloud intrusions and examine various existing cloud-based intrusion detection systems (IDS) in terms of their type, placement, detection approach, and the types of cyberattacks they can detect. In this paper, we have also mentioned some major challenges and limitations of some of the commonly used solutions.

Keywords— Intrusion Detection System (IDS), Cybersecurity, Cyberattacks, Signature, Anomaly, Hypervisor, VM

Number: 10.14704/nq.2022.20.7.NQ33228

Neuro Quantology 2022; 20(7):1811-1820

I. INTRODUCTION

Cloud computing is indeed a contemporary technology that offers shared computational resources through the Internet for data management, storage, and retrieval. It also gives clients with low-cost internet access to numerous applications. It all started in 2006, when Google unveiled the notion of cloud computing. Cloud computing has emerged as the most promising Internet-based technology in the Information Technology (IT) sector in recent years. It is greatly aided through virtualization, which allows for elasticity, scalability, simplicity for usage, and access to a large shared pool of computer resources available throughout the network on-demand. The service-oriented architecture has resulted in a significant change in how services are supplied and maintained.

The National Institute of Standards and Technology defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [1]

Cloud computing is made up of three abstract layers: the system layer which is a virtual machine abstraction of a server, the platform layer that can be understood as a virtualized operating system for the server, and an application layer that has web applications. There are three service models for cloud computing: Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software



as a Service (SaaS). If the provider supports the languages, APIs, and tools required to create applications (such as Google App Engine and Microsoft Azure), then the customers can benefit from the platform where all the applications are developed and then deployed using the PaaS model. IaaS provides services to customers by managing networks, hosting servers, and other resources for clients. Moreover, consumers have total control over whole virtual computers (such as Eucalyptus, Open Nebula). The features of the SaaS model allow the users to unburden them of various tasks like deploying, operating or maintaining software on their workstations. The base layer (IaaS) requires special attention to security since attacks on this layer affect the other levels as well.

Apart from the multiple technologies that it incorporates, such as load balancing, networks, memory management, and operating systems, the dispersed nature of the cloud environment makes it a susceptible and appealing place for attackers to undertake cyberattacks. To maintain their clients' confidence, Cloud Service Provider (CSP) must guarantee the security of their cloud resources. Although various elements of cloud infrastructure offer certain security benefits that can resolve many conventional attacks, still some unidentified threats require countermeasure measures. These elements are virtualization, data segmentation and redundancy, and security centralization. The dispersed nature of the cloud environment makes it the most susceptible and appealing setting for attackers to attempt cyberattacks.

Through methodically evaluating logs, network traffic, and configurations, intrusion detection systems may be used to improve the security of these systems. It is critical in protecting users' data stored in the cloud and preserving customer confidence. Furthermore, traditional intrusion detection systems (IDSs), which are categorised as network-based intrusion detection systems (known as NIDS) and host-based intrusion detection systems (known as HIDS), are not ideal for the modern cloud infrastructures due to the fact that they are not completely able to detect the hidden attack trail. For instance, the network-based IDS might not detect any suspicious events in particular circumstances like encrypted node communication.

Therefore, the attacker might be able to gain control over the deployed virtual servers. [2] [3]

II. TYPES OF ATTACKS IN CLOUD

Regardless of its numerous benefits, migration to the cloud environment creates major security problems as the data being moved to cloud data centres is exposed to security vulnerabilities like confidentiality, integrity, and availability. Furthermore, the continuous availability of cloud technology attracts intruders who seek to obtain access to and exploit the information and applications delivered by cloud service providers. Some of the different types of intrusions or attacks in cloud computing are [3] [4] [5]:

A. Wrapping Attacks

Since it attacked the Amazon cloud in 2009, this is regarded as one of the most significant cloud computing attacks. The primary target of such attacks is the XML signatures, which are signed prior to the message exchange and are meant to protect user credentials. A SOAP message, which contains the destination address in its header part, is generated by the webserver when it receives a request from the client through the virtual machine. This SOAP message is exchanged between the client and the server. Wrapping attacks occur during the processing of soap messages in the Transport Layer Service, after which the attacker can access the cloud. This attack is more akin to a MITM attack.

B. Flooding Attacks

The objective of a flooding attack is to devour cloud resources and damage typical cloud services. The servers in cloud architecture, are set up in such a way that they can readily interact with one another. So, when the load on a single server exceeds its limits, the server can unload itself by shifting part of its work to other servers. It enables the network to process requests more rapidly and in a more dynamic manner. In a flooding assault, the attackers send unnecessary requests to the server through packets known as zombies in order to keep the servers overloaded and busy, forcing the server to shift its responsibilities to other servers. Thereby, processing resources (CPUs) and network bandwidth are depleted, rendering the supply of cloud services to legitimate consumers unprofitable. Any unauthorized party or attacker can take advantage of cloud services via the

Internet and request the VM to execute DoS or Distributed Denial-of-Service (DDoS) attacks. These packets can be ICMP, TCP, UDP, or a combination of the three.

C. Insider Attacks

Insider attacks are carried out by people with varying levels of access to the organization's information and systems. As a result, they may conduct fraud, purposely alter information, or divulge secrets to adversaries. This is fatal since numerous attacks may be carried out from within, and an intruder can readily elude identification if adequate controls are not present. Internal denial-of-service (DoS) attacks are one example of this sort of assault, which is seen as a severe trust issue for cloud systems. For example, an insider executed a DoS attack on Amazon Elastic Compute Cloud (EC2), compromising the confidentiality of cloud users. This raises major concerns about trust within an organization.

D. Denial of Service (DoS) Attack

In DoS attacks, attackers hinder legitimate users from accessing resources and services. The attacker sends the bulk messages to the server from IP addresses that is not legitimate. When the server tries to send a response back, it cannot discover the target address, and the attacker sends repeated incorrect requests to the server before the server kills the connection. In this method, the server will remain busy, and the system will crash after a set length of time.

DDoS: In DDoS, numerous computer systems attack a target, such as a server or a webpage, generating denial of service and resource unavailability. The attackers' goal is to render the website and services unavailable.

E. Port Scanning

The attacker uses port scanning to gather information on open, closed, filtered, and unfiltered ports and to initiate attacks on open ports. A port scanning attack is carried out by delivering designed packets to each port one by one, either sequentially or randomly. This attack allows the attackers to launch these attacks via open ports does but does not directly damage the ports. Port scanning techniques include SYN scanning, UDP scanning, ACK scanning, FIN scanning, TCP scanning, Windows scanning, and so on. Furthermore, attackers can utilise numerous devices to simultaneously scan

different ports in order to maximise their chances of discovering open ports. This method is known as a distributed port scan. This attack aims to compromise the cloud's secrecy and integrity.

F. Malware Injection Attack

The attackers must incorporate their malicious service or code for this attack, which is displayed as one of the instance services. Initially, this attack necessitates the installation of malicious services to run IaaS or SaaS servers. The attacker therefore must manipulate the Cloud system towards considering the new service execution instance among the legal instances for the given service being targeted. When these two phases are accomplished, the cloud is instantly redirected to legitimate user requests to the malicious service. The attacker can then begin code execution, which is usually the primary purpose of such attacks.

G. Backdoor Channel Attack

Backdoor attacks take advantage of software that allows remote access to the system. This type of attacks can be considered as passive attacks. In this attack, firstly the attacker hacks a cloud node and then uses a bot in order to carry out different cyberattacks. When a node is hacked, the attacker gains complete access to the system and data. This attack aims to compromise cloud users' confidentiality and availability.

H. User to Root (U2R) Attack

In this type of attack, the attacker gains access to a legitimate user's credentials before exploiting system loopholes to get root rights. Buffer overflows from a root-level process, for example, can be used to construct root shells. The cloud's integrity is being breached by this intrusion.

I. Virtualization Attack

The most significant necessity is virtualization. The virtual computer will operate on the hardware system directly. The hypervisor is the virtualization control system that manages the hardware resources for the network. This link enables many virtual machines to operate on pooled hardware by detecting the existence of another virtual machine.

III. DETECTION TECHNIQUES

IDS detection approaches that are most commonly employed are based on signatures of known attacks and user activity. However, it is preferable to utilise a combination (hybrid) of these strategies to optimise the performance of IDS.

A. Signature Based Detection

In this detection technique, we compare the information from a particular network or system to that of a signature database. A signature can be understood as a collection of pre-set rules or patterns that correlate to a known attack. This method is often referred to as misuse detection. Few false alarms are used to identify already known attacks. This signature-based method is highly useful in identifying effective breaches, specially for those network managers who have less experience. Its structure allows addition of new signatures to the database without altering the previous ones. Therefore, it is a versatile solution. It cannot, however, identify unknown vulnerabilities.

This method can identify threats at both front-end and the host of the cloud. Installing it at the back end (processing servers) of the cloud can help in detecting both internal and external intrusions. However, it, like traditional networks, is unable to detect unexpected threats in the cloud.

B. Anomaly Based Detection

Anomaly detection compares current user activity to stored profiles of people or networks to detect aberrant behaviour that might indicate an intrusion. Anticipated or innocuous user behaviour can be reflected from either dynamic or static profiles. Training period can be understood as the amount of time required for watching and analysing network connections, behaviour of users, or hosts, in order to construct a profile. Profiles are created by combining numerous information such as unsuccessful login attempts, the number of times a file is viewed by a certain user during a specific period, CPU utilisation, and so on. Detection based on anomalies is efficient for unidentified attackers. A threat discovered using an anomaly-based approach can be utilised as a signature in a signature-based detection system. However, because of erratic network and user behaviour, it generates a huge number of false alerts. Furthermore, huge data sets are required to train the algorithm for user profiles. Using the

anomaly detection approach, unknown attacks in the cloud may be identified at various levels. Due to the vast amount of data flowing via the cloud at many levels (system, network), monitoring breaches becomes tough. Soft computing approaches include:

a) Fuzzy Logic: This logic is based on probability and employs values in the range of 0 to 1. This is for determining the degree of abnormality in the intrusion detected.

b) Artificial Neural Networks (ANN): ANN may be used in intrusion detection to generalise data from faulty data. It is also used to classify data as normal or abnormal.

c) Support Vector Machines (SVM): SVM could be a useful method for detecting intrusions when data samples are restricted and data dimensions do not affect accuracy.

d) Association rules: This method aids in the development of novel signatures that may be used to detect intrusions. Such incursions are made up of well-known assaults or variations on well-known attacks.

e) Genetic Algorithm (GA): The network characteristics chosen by GAs can be used in other approaches to increase IDS detection accuracy. [3]

C. Hybrid Detection

The effectiveness of intrusion detection systems could be greatly increased by integrating signature-based and anomaly-based approaches, that's also known as Hybrid detection. The capacity to identify both predictable and unpredictable attacks utilising signature-based and anomaly-based detection approaches is the impetus for this combination.

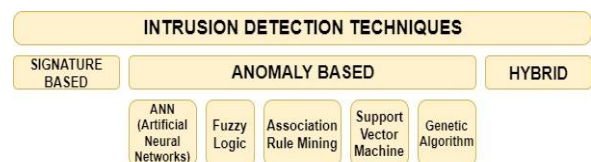


Fig1. Types of Intrusion Detection Techniques

IV. CLOUD BASED IDS

Cloud security is a widely discussed topic, with several solutions offered and still evolving. The traditional cloud infrastructure has numerous loopholes and the possibility of



intrusion. In simple words, intrusion can be described as an act intended to breach a computer's, networks, or cloud systems' integrity, confidentiality, or availability.

Using a cloud-based intrusion detection system is one of the effective ways for preventing such attacks. Cloud IDS (Cloud Intrusion Detection System) detects cloud-native network threats while providing industry-leading cybersecurity. Few different types of cloud-based IDS are [5]:

A. Host based IDS

Host-based intrusion detection systems (HIDS) gather and analyse information from a specific host in order to identify intrusive occurrences. It examines every host activity, including application logs, system calls, and file-system updates, as well as inbound and outgoing packets to and from the host. HIDS analyses this data, and in case there is any change in the system behaviour or application, an alarm is raised, and the network manager is notified further that the system is under attack.

In terms of cloud deployment, HIDS can sometimes be divided into three parts. HIDS can be deployed either in the host OS or in a guest OS within the VM for monitoring. The first case, where the HIDS can monitor either the host or guest OS through communicating over the VMM and is totally within the customer's influence, has the disadvantage of poor attack resistance. It was highly rejected by professionals and researchers and thereby deemed unfit for the virtual cloud. It is only suitable in two scenarios. First, where numerous VMs run on a single process operating on the host. Second, wherein VMM acts as the software of the host machine. On the host system, both normal host processes and the VMM, on which the VM runs, are active.

The best way to enhance the efficiency of HIDS is by providing it with more attributes that it can use as additional information while analysing and detecting threats. However, HIDS in its basic form also requires quite an additional storage for data analysis. Concerning the context of a cloud computing network, HIDS may be deployed on a VM, hypervisor, or host to analyse system logs, user login information, or authorization regulations and identify intrusion activities. The cloud user is in charge

of supervising the HIDS implemented on a VM, whereas the cloud provider is responsible for deploying HIDS on a hypervisor. Although HIDS can analyse encrypted communications, it is vulnerable to DoS attacks and can even be deactivated. HIDS are often employed to secure the integrity of software. Riaz, A. [4] concluded the different types of host-based IDS in his research which was as follows:

DEPLOYE DAT	ATTRIBUT ES	METH OD	CONSTRAIN TS
Each Node [6]	Audit log files, customer profiles	Hybrid	Accurate detection needs more training time, and the number of rules is restricted.
Each Node [7]	Previously known attacks can be detected using the activity records.	Hybrid	The outcomes of the experiments are not provided.
Guest OS [8]	Detecting familiar attack, customer profiles	Anomaly	High-level users spend a greater amount of resources.

Table 1. Deployment of Host-based IDS

However, HIDS hosted on a virtualized environment has the fundamental drawback of being vulnerable to attacks. It gives high system visibility; but, a HIDS does not support virtual machines on the host system. It only functions like a regular HIDS, one that monitors the host system. In combination with other strategies (for example, VMI-based), such a strategy can be effective in safeguarding the host system.

B. Network based IDS

Network-based intrusion detection systems (NIDS) records and analyses the network data to identify potential intrusions. It typically detects intrusions by analysing each packet's IP and transport layer headers. To detect intrusions, NIDS employs an anomaly and/or signature-based detection technique. Signature-based detection analyses network packets and



searches for correlations with signatures of known attacks, whereas for anomaly detection, it compares users' current behaviour in real-time with their previously known profiles.

Another NIDS was proposed in 2010 for the detection of DDoS attacks in virtualized setups, where the NIDS is deployed on a virtual switch. In a typical computer system, this is similar to the standard NIDS and is placed at the boundary server. However, the authors have modified it and tested it for its suitability and usage in a virtualized context [9].

It should be noted that by using a few properly installed NIDSs, several hosts in the network can be protected against intruders. The location of NIDS can be masked from an attacker if it is operated in stealth mode. Attacks on hypervisors or virtual machines in the cloud are detected by deploying NIDS at the cloud server that communicates with the external network. It cannot, however, undertake analysis if the traffic is encrypted, and it cannot identify intrusions within a virtual network confined by a hypervisor. NIDS sensors are usually placed in choke spots. Snort is an example of NIDS. Over the years, researchers have examined the limitations of NIDS when placed at different locations.

On each virtual computer, a NIDS can be installed. The most common method, however, is to deploy it on a virtual switch. This strategy incurs significant computing overhead since one component must tend to the weight of all traffic while also segregating it. Because of its complexity, the IDS may fail in high-traffic settings, rendering all detection findings inaccurate. If the only route for all traffic is interrupted as a result of this, a major DoS attack may occur until the NIDS resumes. NIDS cannot identify internal attacks in the hypervisor as it has limited access of the VM. This results in inability to analyse encrypted communication. On the plus side, a NIDS has a high threat resistance.

C. Hypervisor or VMM based IDS

A hypervisor offers a platform for running virtual machines (VMs). At the hypervisor layer, intrusion detection systems (IDS) are installed. It enables the analysis and monitoring of accessible data in order to spot unusual behaviours and events. The data relies on communication at various levels, such as communication between VM and hypervisor, communication between VMs, and communication within the hypervisor-based virtual network.

DEPLOYED AT	ATTRIBUTES	METHOD	CONSTRAINTS
VSwitch [9]	Acts as SNORT for detecting DoS attacks.	Signature based	Only detects familiar attacks; limited support options for sizeable networks, and IDS glitches can overlook attacks.
Inside of Monitoring VM [10]	Detect only already known attacks.	Signature based	Correlating data from several sensors can have an influence on performance.
PVM [11]	To improve efficiency, separate profiles are created.	Anomaly and Signature based	No prototype.

Table 2. Deployment of Network-based IDS

DEPLOYED AT	ATTRIBUTE	METHOD	CONSTRAINT
PVM [12]	VMM includes a trampoline and hooks function.	The security VM relies on the API (anti-virus) used by the end user.	VMM Code are updated, and trampolines and hooks are bottlenecked.
VMM [13]	Rootkits are detected and identified quickly.	View malware detection based on comparisons	Timing issues while rebuilding views, unable to identify inactive hidden processes, mostly for rootkits
Outside the VMM [14]	Semantic restoration, live monitoring without impacting VMM, and	View malware detection based on comparison	Does not protect from zero-day threats, attacks on the hypervisors might jeopardize approach, and



	benefit for numerous VMMs are all available.	sons	there is a time issue while rebuilding views.
Outside or inside of VMM [15]	Security while logging	Examining logs	There is no virus detection, thus it is time to investigate, record, and playback logs.

Table 3. Deployment of VMM based IDS

VMI or VMM-based approaches are predicated on the assumption that the hypervisor stays safe and non-malicious. However, because VMM's code is tiny and hence less likely to have flaws, this is a commonly accepted premise [16]. According to Modi et al. in [17], the Trusted Cloud Base includes a vSwitch and a hypervisor. The reasons stated were:

1. The code is less prone to errors as it is compact.
2. The introduction of a Trusted Platform Module can improve their security even more (TPM).
3. They are completely under the authority of the cloud service provider.

D. Distributed IDS

A Distributed IDS (DIDS) is a collection of IDSs (such as NIDS and HIDS) that are distributed over a broad network so that they can monitor traffic for suspicious activity. The IDSs on the network can interact with one another or with a centralised server. All of these individual IDSs' has two function components: a correlation manager and a detection component. The detection component monitors the system or subnet and sends the collected data to the correlation manager in a standard manner. The correlation manager is responsible for integrating data from several IDS and providing high-level warnings in response to an attack. The analysis phase employs signature-based and anomaly-based detection approaches, allowing DIDS to identify both known and new attacks.

DEPLOYED AT	ATTRIBUTE	METHOD	CONSTRAINT
Within VM, main module is installed [18]	HIDS and NIDS approaches are integrated, and VM is correlated.	Analysis of anomalies, signatures, horizontal and vertical fusion	There isn't any prototype.
One module is contained within VMM, while the other is external. [19]	Semantic restoration, low expenses	Anomaly	Execution is halted in the event of an event, there is no defensive mechanism, and only rootkits are used.
Processing Server [2]	Signature-based authentication, auditable log files, and client profile.	Hybrid	There is no application.
Each and every cloud area [20]	Can identify known attacks based on their signatures	Signature	High computing overhead, as well as the inability to identify unexpected attacks

Table 4. Deployment of Distributed IDS

E. Perimeter IDS

It recognizes and identifies the placement of intrusion tackle on the peripheral of critical facilities. The perimeter is fenced with fibre optic cable. When a disturbance on the fence is detected and considered, an alert is triggered. Host-based intrusion.

V. CHALLENGES

Intrusion detection algorithms have developed as networks and computer architecture have evolved, with the purpose of providing security and protection. Despite the substantial study, there are still unresolved issues in this field. Limited detection efficiency, absence of common metrics & evaluation methodology, low throughput & high-cost IDS, and encrypted data are some of the major problems in implementing an intrusion detection system. Low detection efficiency is caused by a high false-positive rate. In anomaly-based intrusion detection systems, less training



time results in more false positives, whereas greater training time results in increased resource use. It is necessary to strike a balance between the two elements, namely security and usefulness. In wideband technology, large data rates (Gbps) result in limited throughput and high IDS costs.

Grid computing-based and distributed detection schemes have been proposed to address this issue. Due to a lack of common criteria and assessment procedures, selecting IDS is a complex task. IDS are targeted and no countermeasures are in place to safeguard them. Encrypted data is one of the most significant challenges that IDS encounter across all platforms. The aforementioned considerations should be taken into account while creating and implementing an IDS [21].

1. Secure Hypervisor

The hypervisor on which the virtual machines are housed has a significant impact on cloud security. Many virtual machines (VMs) can be hosted by a single hypervisor simultaneously. But this creates a situation where several VMs are on a single VM working on a hypervisor might get hacked. It is not guaranteed that hypervisor cannot be accessed by the intruders and, as a result, all of the VMs that operate on it. A hacked hypervisor can jeopardise a perfectly secure VM. As a result, during the service level agreements give rise to a couple of important questions like: How are VMs isolated? What will the cloud provider's response be? How is a security flaw in a hypervisor discovered? Implementations of a secure hypervisor include sHype and NoHype.

2. Lack of dataset

Attacks against cloud computing have grown in recent years, and it has been seen that a lack of datasets makes it difficult to construct an effective intrusion detection system. Because of the varied operating systems deployed in virtual machines, the diversity of user needs, and the amount of cloud data, the existing datasets used for traditional computing cannot be employed. The true and false positive rate of an intrusion detection dataset determines its efficacy. A genuine positive rate can be attained by assessing the number of attacks detected by the

cloud IDS after sending multiple cyberattacks to it. The false-positive rate defines the false alert ratio. An ideal IDS will have a false positive rate of zero, which means that no false alerts are created.

3. VM Migration

The current research on the potential influence of virtual machine migration on cloud intrusion detection systems is sparse. Through a heap, stack, or integer overflow vulnerability present in migration module, attackers can acquire complete control of a VM during the migration process. Furthermore, without suitable rules, an intruder can commence or stop the VM migration process, resulting in a denial of service. It can also result in insertion of malicious code apart from obtaining control of the VM during migration. It should also be noted that unsecured channels utilised during migration provide an opportunity for the attacker to perform active and passive attacks [4].

VI. CONCLUSIONS

IDS ensures the confidentiality, integrity, and availability of a computer system. IDSs for cloud computing are in high demand due to the exponential rise of cloud users. For the Cloud computing paradigm to be successful, its security must be prioritized. In this study, we discussed numerous intrusions that influence cloud CIA as well as existing methods for cloud intrusion detection. Then we thoroughly showed several forms of IDS in a cloud setting. There is also a full overview of several intrusion detection strategies. We've included a summary in the format of figures and tables to assist in grasping the entire scenario. IDS is the most effective method for detecting intrusions and enhancing cloud security. We examined some of the most recent research efforts that were offered to improve cloud security through the use of intrusion detection systems (IDS). According to the findings, while many IDS approaches have been offered to aid in the detection of cloud intrusions, they do not guarantee total protection. As it can be seen that almost every individual design lacks in some aspect, the most appropriate solution would be to use a combination of several detection mechanisms to attain the necessary level of security in the cloud environment. Soft

computing solutions can significantly improve cloud security. However, there are a number of obstacles and unresolved concerns that must be addressed.

REFERENCES

- [1] Alturfi, S.M., Muhsen, D.K., Mohammed, M.A., Aziz, I.T. and Alshamee, M., 2021, February. A Combination Techniques of Intrusion Prevention and Detection for Cloud Computing. In *Journal of Physics: Conference Series* (Vol. 1804, No. 1, p. 012121). IOP Publishing.
- [2] Shelke, M.P.K., Sontakke, M.S. and Gawande, A.D., 2012. Intrusion detection system for cloud computing. *International Journal of Scientific & Technology Research*, 1(4), pp.67-71.
- [3] Mehmood, Y., Shibli, M.A., Habiba, U. and Masood, R., 2013, December. Intrusion detection system in cloud computing: Challenges and opportunities. In *2013 2nd National Conference on Information Assurance (NCIA)* (pp. 59-66). IEEE.
- [4] Riaz, A., Ahmad, H.F., Kiani, A., Qadir, J., Rasool, R. and Younis, U., 2017. Intrusion detection systems in cloud computing: A contemporary review of techniques and solutions. *Journal of Information Science and Engineering*, 33, pp.611-634.
- [5] Devi, B.T., Shitharth, S. and Jabbar, M.A., 2020, March. An Appraisal over Intrusion Detection systems in cloud computing security attacks. In *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)* (pp. 722-727). IEEE.
- [6] Vieira, K., Schulter, A., Westphall, C. and Westphall, C., 2009. Intrusion detection for grid and cloud computing. *It Professional*, 12(4), pp.38-43.
- [7] Dhage, S.N. and Meshram, B.B., 2012. Intrusion detection system in cloud computing environment. *International Journal of Cloud Computing*, 1(2-3), pp.261-282.
- [8] Lee, J.H., Park, M.W., Eom, J.H. and Chung, T.M., 2011, February. Multi-level intrusion detection system and log management in cloud computing. In *13th International Conference on Advanced Communication Technology (ICACT2011)* (pp. 552-555). IEEE.
- [9] Bakshi, A. and Dujodwala, Y.B., 2010, February. Securing cloud from ddos attacks using intrusion detection system in virtual machine. In *2010 Second International Conference on Communication Software and Networks* (pp. 260-264). IEEE.
- [10] Roschke, S., Cheng, F. and Meinel, C., 2009, August. An extensible and virtualization-compatible IDS management architecture. In *2009 Fifth International Conference on Information Assurance and Security* (Vol. 2, pp. 130-134). IEEE.
- [11] Gupta, S., Kumar, P. and Abraham, A., 2013. A profile based network intrusion detection and prevention system for securing cloud environment. *International Journal of Distributed Sensor Networks*, 9(3), p.364575.
- [12] Payne, B.D., Carbone, M., Sharif, M. and Lee, W., 2008, May. Lares: An architecture for secure active monitoring using virtualization. In *2008 IEEE Symposium on Security and Privacy (sp 2008)* (pp. 233-247). IEEE.
- [13] Jones, S.T., Arpaci-Dusseau, A.C. and Arpaci-Dusseau, R.H., 2008, March. VMM-based hidden process detection and identification using Lycosid. In *Proceedings of the fourth ACM SIGPLAN/SIGOPS international conference on Virtual execution environments* (pp. 91-100).
- [14] Jiang, X., Wang, X. and Xu, D., 2010. Stealthy malware detection and monitoring through VMM-based "out-of-the-box" semantic view reconstruction. *ACM Transactions on Information and System Security (TISSEC)*, 13(2), pp.1-28.
- [15] Dunlap, G.W., King, S.T., Cinar, S., Basrai, M.A. and Chen, P.M., 2002. {ReVirt}: Enabling Intrusion Analysis Through {Virtual-Machine} Logging and Replay. In *5th Symposium on Operating Systems Design and Implementation (OSDI 02)*.
- [16] Tupakula, U., Varadharajan, V. and Dutta, D., 2012, December. Intrusion detection techniques for virtual domains. In *2012 19th International Conference on High Performance Computing* (pp. 1-9). IEEE.



- [17] Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A. and Rajarajan, M., 2013. A survey of intrusion detection techniques in cloud. *Journal of network and computer applications*, 36(1), pp.42-57.
- [18] He, J., Tang, C., Yang, Y., Qiao, Y. and Liu, C., 2012, December. 3d-ids: IaaS user-oriented intrusion detection system. In *2012 Fourth International Symposium on Information Science and Engineering* (pp. 12-15). IEEE.
- [19] Ibrahim, A.S., Hamlyn-Harris, J., Grundy, J. and Almorsy, M., 2011, September. Cloudsec: a security monitoring appliance for virtual machines in the IaaS cloud model. In *2011 5th International Conference on Network and System Security* (pp. 113-120). IEEE.
- [20] Lo, C.C., Huang, C.C. and Ku, J., 2010, September. A cooperative intrusion detection system framework for cloud computing networks. In *2010 39th International Conference on Parallel Processing Workshops* (pp. 280-284). IEEE.
- [21] Elmasry, W., Akbulut, A. and Zaim, A. (2021) A Design of an Integrated Cloud-based Intrusion Detection System with Third Party Cloud Service. *Open Computer Science*, Vol. 11 (Issue 1), pp. 365-379.