PROVIDING SECURITY TO DIGITALIZED INFORMATION USING INTRUSION DETECTION SYSTEM

T.Aswani[1]., B.Nandini[2]., C.Sathwika[3]., K.Jyothirmai[4] ., V.Aruna Sri[5]
1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉ aswani.thummalagunta@gmail.com)
2, 3, 4, 5 B.Tech CSE, (19RG1A05C7, 19RG1A05D2, 19RG1A05F0, 19RG1A05H7),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract
Users that rely on the cloud for their infrastructure, apps, and data storage can benefit from following security best practices. Therefore, the goal of cloud security is to prevent unauthorized access to data and infrastructure by ensuring its privacy, integrity, availability, and prompt detection of intrusions. The primary goal of an IDS is to detect malicious activity in order to keep sensitive user information and cloud services safe. Therefore, this research presents a unified perspective of current security solutions, including their benefits and drawbacks. It covers the IDS state-of-the-art, the relevance of feature selection and dimensionality reduction, and cloud service model-specific security considerations. This study organizes IDS methods by the kind of threats they detect, where they are deployed, and how they are set up. Strategies for introspecting both the host operating system and guest operating systems (VMI and HVI, respectively) will also be investigated. Concerns about cloud security, the significance of feature selection, and an examination of current IDS approaches form the study's organizational pillars. Finally, this paper provides a summary of current security problems/challenges and research needs to be filled in the future.

Introduction ;

User services such as apps, infrastructure, and storage are all made available via cloud computing. Over the internet, a cloud user may access and modify hardware and software as needed. While there are numerous advantages to using cloud computing, there are also certain disadvantages and difficulties to be aware of. Cloud computing presents a number of issues, including those of security, privacy, load balancing, pricing, and performance management. Since user information and apps are located in the cloud, security is the most pressing concern. Policies and procedures are what make up cloud computing security, which is what keeps your information, apps, and hardware safe in the cloud and out of the wrong hands. SQL injection, cross-site scripting, and flooding attacks are also prevented by this method (Khalil et al., 2014; Rong et al., 2013). In addition, cloud users and service providers often report security vulnerabilities as a result of a wide range of assaults. In 2012, for instance, VUPEN Security uncovered a VM escape exploit (Mimiso, Sept. 2012). DropboX also suffered a distributed denial of service (DDoS) assault in 2013 that resulted in a 15-day outage for all customers (Marinos, 2013). According to Symantec (2015), more than 450 vulnerabilities, including zero-day exploits, were revealed in January 2015. Over 650 million cyberattacks were launched against cloud users in 2018. Addi Attacks against containers and cloud services, as well as targeted ransomware, complex phishing operations, and DDoS campaigns, were common in 2019. Intruder alarm or IDS for short. Cloud services may be further subdivided into Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). There are unique risks and complications associated with each of these services and methods that must be addressed in order to ensure user safety (Khraisat et al., 2019; Modi et al., 2013). For instance, IaaS is susceptible to VM image attacks, VM network assaults, hypervisor attacks, DNS poisoning, ARP/IP spoofing, XSS attacks, and data attacks (Aldribi et al., 2020; Jebamalar et al., 1882; Kirat et al., 2014; Prabadevi et al., 2020); PaaS is susceptible to phishing attacks, Man-in-the- Therefore, we need a system that can defend itself against intrusion and other forms of harmful activity. This is why cloud security specialists have created intrusion detection systems. Intruder Detection Systems (IDS) may be either host-based or network-based. HIDS keeps an eye onChoosing Features in Version 1.1The detection accuracy of the system and the FAR may both be improved by the use of feature extraction, which is a method of data reduction. Data volume, variety, and velocity have all skyrocketed as a consequence of the explosion of network endpoints. Keeping and processing this data is essential for making effective use of it. However, it is certain to slow down the entire procedure if these data are sent directly into the IDS module. Raw audit data of network traffic is not ideal for this purpose since not all characteristics help in detecting an intrusion. According to a study by Zhang et al. in 2020, each network packet has 41 characteristics, leading to a total of 241 -1 subsets. Managing such a vast number of subsets is difficult since doing so demands a lot of memory and increases the cost. Network traffic characteristics are further classified as irrelevant, weakly relevant, or important for intrusion detectionthe right, or quite relevant. In order to improve the system's efficiency and precision, the raw data must undergo pre-processing to reduce dimensionality and get rid of the irrelevant features. Using a process called feature selection, only the feature(s) that provide the most faithful representation of the original data should

be retained. Using this technique, just the characteristic that best represents the original data is kept. The system's effectiveness depends on the features used for intrusion detection, thus this must be done with caution. Several academic research groups have devoted significant time and energy to the development of various algorithms for feature selection. Khammassi and Krichen (2017) offered a GA-based approach to feature selection. Experts in the field of domain expertise are required, according to them, since "deciding upon the right set of features is a difficult and time-consuming process." This highlights the need for a technique that can automatically choose the most advantageous characteristics.

1.1.1. Strategies for Selecting Important Attributes Several feature selection techniques are presented in the literature with the goal of improving system performance while decreasing resource use. Zhang et al. (2020) introduced a feature-selection-based IDS to improve detection accuracy and efficiency. Prasad et al. 2019 presented an IDS technique based on feature selection. The number of features was reduced by half thanks to rough set theory. They proved that feature selection may reduce complexity and improve performance. Selecting features may be done in a few different ways, the most popular being the Filter Method, Wrapper Method, and Embedded Method.Method of I-Filters

When it comes to choosing features, this is the benchmark. In this technique, characteristics are either maintained or eliminated according to a predetermined cutoff value. It has been shown that The procedure is carried out in-data. Although its price is lower than that of competing systems, its performance worsens if redundancy is low. Rawashdeh

Using the TShark tool, & Al-kasassbeh (2018) analyzed network traffic and retrieved characteristics for the IDS.

"I-wrap" technique

Computing feature subsets that sufficiently represent the data is the first stage of this three-stage approach. We then use an objective function to rank and classify these subsets. Finally, an ideal feature subset is chosen to improve the system's accuracy (Khammassi & Krichen, 2017). Wrapper techniques outperform filters but need more work to set up and maintain. Khammassi and Krichen (2017) introduced a GA-LR wrapper technique for feature selection in network intrusion detection.

.

I've Combined Various Approaches During the course of model training, the optimal subset of features is automatically determined by the system. This method is faster than filtering and wrapping because of this. Embedded methods often include penalization strategies for feature selection, and least absolute shrinkage and selection operator (LASSO) for regression. Embedded techniques have grown in popularity because to their low computing cost and robustness against over-fitting. Patil et al. (2019) developed an NIDS by using a feature selection technique. In this setup, we used a binary bat technique for feature reduction, which included two fitness functions. They reduced the number of traffic controls from 44 to 26. Eliminating features improved the system's accuracy. Similar to how Rawashdeh and Al-kasassbeh (2018) and Sakr (2019) used Particle Swarm Optimization (PSO) for feature selection. Both approaches showed enhanced anomaly detection capability, with better detection accuracy and reduced FAR. They demonstrate the importance of feature selection by doing a comparative analysis. The Effectiveness of Interventions Dataset

Evaluating the efficacy of an intrusion detection system requires a dataset that accurately represents real-world network activity. Several datasets have been used by researchers throughout the years. These include KDD99, NSLKDD, and ISC2012 (Citation, 2016; Subhy & Basheer, 2018; Thampi et al., 2019). Because of inconsistencies and gaps, these datasets do not accurately represent the system's actual performance. Due to record redundancy, the categorization results are skewed in favor of the repeated records. Therefore, it was necessary to have a dataset that dealt with the aforementioned problems. To evaluate the performance of IDS, Moustafa and Slay developed the UNSW-NB15 data set in 2015. This set of traffic statistics, which includes both regular occurrences and outliers, is complete and free of errors. By contrasting the outputs of two separate applications, Ar- gus and Bro-IDS, 47 features were generated for each record in this dataset. The results of these tools were stored in a SQL database and matched based on flow criteria such as Source/Destination IP address and port number and Transaction Protocol. After that, data are categorized as normal or abnormal. A value of 0 represented a normal entry, while a value of 1 represented an extreme one. While there have been many enhancements since the last time this dataset was used, it still does not adequately represent the environments that have been the target of recent assaults.

To fix UNSW-NB15, Sharafaldin et al. (2018) developed CICIDS2017 and CSE-CIC-IDS-2018. Recent incidences and statistics are included in these data sets, which also indicate ongoing trends. There has been use of both the victim's network and the attacker's network. Six types of attacks are covered by CICIDS2017 and CSE-CIC-IDS-

2018, including brute force, heartbleed, botnet, DoS/DDoS, online assault, and penetration. These datasets were developed in two phases. First, 80 flow-based features were extracted from the pcap file. A random forest regressor was then used to determine which of the 80 attributes were most useful. Important features are ranked using machine learning techniques. They provide a comparative study of their efforts by comparing the recommended datasets to previously collected data.

1.1. 1.1 Khraisat et al. (2019) offer a thorough introduction to the aspects of the dataset.

1.2. Additionally, many efforts have been made over the last decade to address privacy and security problems in cloud secu- rity. Based on their findings, researchers recommend focusing greater resources on intruder detection systems to protect cloud infrastructure, applications, and user data from attacks. Therefore, the purpose of this work is to provide a comprehensive review of existing IDS techniques, including a categorization and analysis of these methods, a discussion of their advantages and disadvantages, a summary of common types of attacks, an examination of the significance of feature selection in IDS methods, and a survey of the various datasets currently at our disposal. We will also call attention to research gaps and new directions in the area that hold promise for progress. The objectives of this research are summarized below.

1.3. The purpose of this research is to examine the state of the art in intrusion detection systems (IDS). We have organized IDS techniques into five categories according to the following criteria: Signatures are used in (1)

1.4. IDS (2) Anomaly-based intrusion detection systems Third-party virtual machine introspection (based), fourth-party hypervisor introspection (based), and fifth-generation hybrid intrusion detection systems are all possible.

This study's secondary objective is to stress the value of picking the right features. To further improve the overall accuracy and efficiency of the intrusion detection system, we also give a summary of security vulnerabilities and attacks in cloud service models.

The study also looked at the current research gaps and future research trends to improve security and privacy.

The Importance of Cloud Security

Due to the nature of Internet delivery, cloud services introduce new security risks for both the provider and the user. The following sections highlight some potential threats to the security and privacy of cloud infrastructure.

The most crucial part of cloud security is the data center where customers' data and apps are kept.• For privacy considerations, cloud service providers do not let their customers to implement their own security solutions at the management layer.

2. the goals and outlook for the project. Security and privacy risks are exacerbated in cloud computing because of its reliance on virtualization and its users' sharing of a common pool of resources.

Thirdly, attacks pose the greatest danger to the safety of cloud service providers. These might come from the service provider itself or from the customer themselves. Therefore, it is crucial to set up a system that can protect you from hackers and other dangers.

4. The remaining sections of the paper are organized as follows: Section 2 covers discussions on related research. In Section 3, we briefly review the search techniques and published literature used to locate potentially applicable contemporary approaches. In Section 4, we take a look at the different IDS techniques that are in use today. In Section 5, we will offer our results and discussion based on a number of criteria, and in Section 6, we will engage in a discussion of open questions and developing themes. In Section 7, we draw conclusions.

The Meaning of Six Surveys Our own survey design was informed by the aforementioned research material. Confidentiality, availability, and integrity are the three pillars on which cloud security rests, as discussed by Zhou et al. (2010), Modi et al. (2013), Denz & Tay- lor (2013), and many others. Other works have focused on specific aspects of cloud security, such as cloud resilience, malware, and virtual machine security.

2. supervisor (VMM), Khan (2016) provided a threat model for many assaults and their remedy, whereas Pandeeswari and Kumar (2015) investigated commonplace assaults and how machine learning may handle them. These surveys didn't ask about how to fix cloud security issues.

3. Furthermore, Alhenaki et al. (2019) discussed potential dangers in IaaS, PaaS, and SaaS. Extensive details were provided on data theft, data breaches, malicious insiders, accounts and services being hijacked, etc. The many security attacks and their countermeasures are discussed in this article as well. Eight common threats to cloud security, privacy, and availability were highlighted by Jebamalar et al. in 1882. Different types of attacks, attack vectors, attack surfaces, threats, and vulnerabilities were discussed in this article as they pertain to cloud security. Security concerns specific to cloud computing were also discussed. The problem is that, like other efforts to address cloud computing security issues, it fails to provide particular security procedures. However, a literature evaluation of the IDS was published by both Arjunan & Modi (2017) and Azeez et al. (2020). Signature-based IDS, anomaly-based IDS, and hybrid techniques are discussed, however neither article takes into consideration VM Introspection (VMI) or Hypervisor Introspection (HVI).

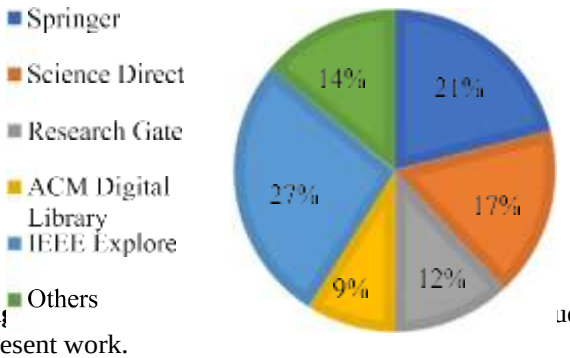
4. Third, when we looked at the big picture of the surveys that were relevant to our issue, we saw that many of them covered ground such as cloud computing security, cloud

threats, intrusion detection systems, and intrusion prevention systems. The intrusion detection techniques of VMI and HVI were not included in any of the aforementioned research projects. Another significant shortcoming of all the research in this area is that feature selection and datasets have not been taken into consideration in any survey. Methods for selecting features might improve the system's efficiency and accuracy while decreasing the total cost of security. Because of this, the research highlights the well-established IDS techniques, feature reduction, and datasets. We'll evaluate this research against the other polls here using the same standards. In Section 5.4, we compare our findings.

5.

Research Methods Monographs Volume 10To create this research, we used the systematic review methodology established by Kitchenham et al. (2009) and Charband & Navimipour (2016). The major goal of this research is to compare and contrast the different IDS approaches that are presently in use. Several methods exist for securing cloud infrastructure, and they should all be evaluated in light of the unique dangers they confront. In this study, we present and explore a variety of strategies for assuring security at various levels of cloud architecture. We searched academic journals, conferences, and other publications from January 2010 through June 2020 for the papers that formed the basis of this study. **securing the cloud as a priority. These include Google Scholar, the ACM Digital Library, IEEE Xplore, and Springer's ScienceDirect and Scopus.**

A list of terms for locating individual articles in the aforementioned literature has also been developed. Cloud security challenges and responses to such vulnerabilities are the focus of the following glossary words. Some of the most common topics discussed in relation to cloud computing include: security, intrusion detection, intrusion prevention, feature selection, the necessity of dimensionality reduction, assaults, security difficulties, and datasets. We used abstracts to determine which publications were relevant to our study and which could be disregarded. By reviewing and analyzing a variety of relevant papers, we want to provide a complete overview of the IDSs now accessible in cloud computing. The breakdown of research strategies and tools is shown in Figure 1.Intrusion Detection Systems in the Cloud: Current DevelopmentsIn this study, we classify and rate a wide variety of intrusion detection techniques. This research classifies IDS techniques in terms of deployment, environment, and attacks. Five different kinds of detections



6.

Fi uded in present work.

seen in the second figure. More detailed discussions of these techniques are provided below. Tables 1 through 5 further outline key features and limitations of the present IDS approach.

Signature-Based Intrusion Detection: A Real-World ExampleNetwork traffic is analyzed for malicious behavior by signature-based intrusion detection systems, which compare it to known patterns or malicious code. It maintains a signature database to monitor attacks and other forms of violence. This signature database must be routinely updated in order to detect sophisticated attacks. Malicious conduct may be uncovered by comparing freshly received network packets to the previously defined rules. Snort, introduced by Martin Roesch (2015), is a signature-based approach that is both accessible and popular. The IDS that uses packet capture and signature matching Use of Snort is pervasive.and ongoing analysis of network performance. The main parts of the system are shown in Fig. 3 and include the packet decoder, pre-processor, detection engine, logging and warning system. After being preprocessed, freshly obtained traffic is sent to the detection engine. During pre-processing, we remove redundant or unaccounted-for data. The next thing that happens is the detection engine compares the current packet to the signatures it has stored. A notification is issued to the proper authorities if a match is detected; otherwise, the packet is permitted to continue its journey unchanged (Roesch, 2015).

Many academics have presented signature-based IDS, but Lin et al. (2012) proposed a rule-based NIDS to detect known threats in a cloud setting. Information is collected and constantly updated from each VM's operating system to establish the detection criteria. Collaborative intrusion detection was first made possible by a CGA presented by Lo et al. in 2010. Each server has an intrusion detection system (IDS) installed, which consists of a signature database and a block table that records attacks. Before looking for signatures, Snort first verifies the packet against a block table. Recent attacks should be prioritized for investigation because of their higher likelihood. By setting a threshold, alert clustering can tell you how serious an abnormal packet is. Then the IDS system will automatically delete the malicious packet. The use of signatures in IDS approaches was also proposed by Meng et al. (2014). When dealing with malicious network traffic, the authors argue, the chance of a mismatch is greater than the likelihood of a match. So they used a mismatch policy to identify the breach. Mandal et al. (2015) proposed using signature-based intrusion detection systems to spot application-level attacks. A sniffer is placed between the

cloud provider and the client in this setup.

SNORT-based network intrusion detection system for open-source cloud infrastructure. The author built an NIDS to categorize assaults and discovered that a Denial of Service (DoS) attack could be carried out through a UDP deluge. The suggested system's performance was measured using an OpenStack-based private cloud. For the MapReduce architecture, Aldwairi (2017) demonstrated a signature-based IDS based on the Myer algorithm. They employed a CPU with many cores to speed up the signature-matching process while using less memory. An overview of current signature-based IDS methods is provided in.

10.1 anomaly detection IDS.Signature-based IDSs can quickly identify common threats with a low false positive rate, but they need to have their signature databases updated often. Anomaly detection methods were created to address the shortcomings of signature-based IDS. In order to construct a user profile, this method analyzes their actions. This behavioral profile is then utilized to detect both common and uncommon forms of assault. Fig. 4 is a simplified schematic of one possible anomaly detection method. The first part is spent learning how to detect, whereas the second is spent actually finding things. During the training stage, the feature creation module gathers data from the host system or network and performs preliminary processing to build features. The characteristics are utilized by the training module to create a model of behavior. This approach classifies information as either typical or suspicious. This model is used during the anomaly detection phase to find possible points of entry. The system automatically notifies the security administrator of any abnormalities in traffic (Sari, 2015). The increased computational power is worth it so that innovative assaults may be thwarted by this method. Any unusual behavior triggers an alert, and it's the security manager's job to figure out why. Detection methods for anomalies like Machine Learning, Fuzzy Logic, Support Vector Machine, and Data Mining lead to other categorizations of anomaly-based methods.

After running numerous ANNs, the results are combined using the fuzzy part. According to the findings, this method is very effective in detecting a variety of hyper- visor attacks with low false positive rates. The combination of PSO and ANN was also employed by Rawashdeh & Al-kasassbeh (2018). Where PSO determines the optimal weights for the

Several research have investigated these methods in the last decade. To create their behavioural model, Kumar et al. (2011), for instance, used a hidden Markov method. This method use a log file containing the frequency of system calls to identify suspicious actions. Three distinct profiles, representing different levels of recent activity, are used to build an IDS. The low profile represents patterns with a little chance of matching. However, the high profile is associated with patterns that have an extremely high probability of being a match. The current profile, which is in the center, is a partial match. Each profile is compared to a fixed criterion.

A machine-learning technique called static program behavior analysis was introduced by YuXin (2011). Decoding programs is the first stage, followed by the development of a context-free language to characterize the workflow. We constructed the whole sequences by searching and assembling all of the possible variants. All system calls have been condensed into a handful of basic steps. Information Gain (IG) and Document Frequency (DF) were used as feature selection methods. Combining unsupervised learning with supervised classification, Srinivasan et al. (2012) developed an IDS approach employing a two-tier system. Wolthusen (2012) developed a method for detecting intrusion based on the frequency of regular vs aberrant system calls. To begin, a massive amount of data is accumulated from each VM over a lengthy period. After startup, the methos operates on the assumption that the VMs are not malicious. When measured in lines, its temporal complexity is O (n). This method detects everything with a false-positive rate of just 11%.

To identify unanticipated assaults in the cloud, SyedNavaz et al. (2013) presented an entropy-based intrusion detection system. To identify assaults with low frequency A system call-based anomaly detection method was developed by Gupta and Kumar (2015). This approach avoids the need for a training system by creating a database of system calls according to the specifications of a given set of keys. One key stands for the name, while the other shows the next in line for execution. The baseline database is produced by comparing the current state to an earlier time period.

neural network to achieve optimal performance. To enhance the precision of the system, Zhang et al. (2020) used the integrated dominance algorithm (MaOEAABC) with fea- ture optimization approaches. On the premise that harmful behavior is obviously distinct from normal behavior, Deshpande et al. (2014) presented host-based intrusion detection systems (HIDS). In order to identify infiltration, this method tracked system call failures using k-NN. With ANN, Catillo et al. (Intelligence et al., 2020) used a two-tiered

strategy in order to label the many types of attacks that occur. In this configuration, the ANN consists of three layers: the input and output layers are the same size, but the hidden layer is often much smaller than the input. The hidden layer is responsible for capturing crucial aspects of the training data. By learning from past results, this method may improve accuracy to 99 percent at the second level while incurring just 0.5 percent FAR. For the purpose of intrusion detection, Aldribi et al. (2020) presented both an anomaly detection method and an instance-oriented feature extraction method. In Table 2, we can see the benefits and drawbacks of different methods.

CONCLUSION

security vulnerabilities and hacking attempts in cloud computing service models were discussed. As a consequence of these actions, data theft, account takeovers, malware injection, insider assaults, database manipulations, and denial-of-service/distributed denial-of-service attacks (DoS/DDoS) occur. By offering Confidentiality, Integrity, Availability, and real-time intrusion detection, Security in the cloud safeguards cloud-based data, applications, and infrastructure against unauthorized access. To help keep you safe from hackers, researchers created an intrusion detection system (IDS). In this paper, we provide a classification model based on the IDS configuration, its location, and the threats it detects after analyzing 43 publications on current intrusion detection approaches. Select articles published between January 2010 and June 2020 are discussed, both for and against. Attacks across all service types (IaaS, PaaS, and SaaS), and datasets for performance assessment of cloud IDS, have all been covered in this article. We have also examined the significance of feature selection and dimensionality reduction in the intrusion detection process and their ability to boost the system's overall performance. Different IDS methods, together with their benefits and limitations, are compared and contrasted. Finally, certain unanswered questions have been raised that will have to be investigated in other studies. Various IDSs were created in the literature, each using a unique set of methods. However, it is challenging to integrate all areas of security simultaneously, especially with the rise in hostile activity, so there is always room for improvements. That's why scientists need to study ways to boost intrusion detection by combining existing methods. In order to boost system performance and detection accuracy, future studies should investigate feature selection and optimization strategies. Furthermore, we have addressed several directions for future research to take in order to enhance cloud security without adding to the cost.

References

Cloud-Based Intrusion Detection and Prevention System for Collaborative Security, 2022.

In a virtualized cloud computing environment, A.K.M. A, Virtual machine introspection based spurious process identification, (2016).

(2020) Ahram, T., Karwowski, W., Vergnano, A., & Leali, F.Integration of Human and Intelligent Systems, 1131, Advances in Intelligent Systems and Computing, 2020.

A. Al Mamouni, M. Hanoune, & Z. Al Haddad (2016), On August 8th, 2016 we published a collaborative network intrusion detection system (C-NIDS) for use in the cloud.

According to Aldribi (2020), Traoré (2020), Moa (2020), and Nwamuo (2020).Online multivariate statistical change tracking for computer- and security-hypervisor-based cloud intrusion detection, 88 10.1016/j.cose.2019.101646.

(2017). Aldwairi, M.Myers method for signature matching in IDS utilizing the MapReduce architecture, 10.1186/s13635-017-0062-7.

In 2019, Alhenaki, Alwatban, Alamri, and Alarifi published their findings. A look at the current state of cloud security. Computer Applications and Information Security: Second International Conference, ICCAIS 2019, Proceedings, pages 1-7, 2019. 10.1109/CAIS.2019.8769497. In 2017, Arjunan and Modi published their work. In order to better secure the network layer in the cloud, a new intrusion detection framework has been developed. In ISEASP 2017: Proceedings of the ISEA Conference on Security in the Asia-Pacific. 10.1109/ISEASP.2017.7976988.

Adewumi, A., Van der Vyver, C., Ahuja, R., Azeez, N. A., Bada, T. M., Misra, S., and Azeez, N. A. What you need to know about intrusion prevention and detection systems now. Intelligent Systems and Computing Advances, Volume 1042, Issues 685–696. 10.1007/978-981-32-9949-8_48.

(2019) V. Balamurugan and R. Saravanan. Improved cloud-based IDS/IPS using hybrid classification and out-of-the-box (OTS) rule development. 22(130):13027-13039, Cluster Computing. 10.1007/s10586-017-1187-7.

Matthews, C.; Benninger, C.; Neville, S. W.; Yazir, Y. O.; Coady, Y. (2012). Maitland, less resource-intensive virtual machine introspection to enhance cloud security. IEEE's 5th International Conference on Cloud Computing Proceedings Pages 471–478 of CLOUD (2012). 10.1109/CLOUD.2012.145.

Sun, W.; Bharadwaja, S.; Niamat, M.; and Shen, F. (2011). Collabra, Collaborative intrusion detection using the Xen hypervisor. Published in the New Generations in Information Technology Conference Proceedings Pages 695–700 in ITNG 2011.

10.1109/ITNG.2011.123.
(2019) Borisaniya and Patel. Towards a Cloud Security Framework based on Virtual Machine Introspection. Sādhanā, 44, 1-15. 10.1007/s12046-018-1016-6.2013.
As of 2016, Charband, Y., and Navimipour, N.J.A systematic literature analysis of the current state of the art and suggestions for the future of online knowledge exchange platforms, 10.1007/s10796-016-9628-z.
In 2016, Chiba, N. Abghour, K. Moussaid, A. El Omri, and M. Rida published their findings. A collaborative and hybrid cloud-based intrusion-detection system built on snort and an improved version of the back-propagation neural network. Twelve Hundred and Sixteen in Procedia - Computer Science. 10.1016/j.procs.2016.04.249.
Empirical Studies (2016).Between 2010 and 2015, researchers analyzed 0-21 of the KDD99 dataset for use in intrusion detection and machine learning.
Taylor, S., & Denz, R. A literature review on cloud computing safety. 2(1):1-9 (10.1186/2192-113X-2-17), Journal of Cloud Computing.
(2014). Deshpande, P., S.C. Sharma, S.K. Peddoju, and S. Junaid.HIDS is a host-based intrusion detection system designed specifically for use in a cloud computing infrastructure. 10.1007/s13198-014-0277-7.
Y. Lin, Y. Wu, Y. He, & B. Ding (2013). HyperVerify is a hypervisor monitoring framework that makes use of virtual machines. 7th International Conference on Software Reliability and Enhancement (SERE-C 2013) Companion (pp. 26-35). Proceedings. 10.1109/SERE-C.2013.20.
According to Ficco (2016), Tasquier (2016), and Aversa (2016). Federation cloud intrusion detection. Computational Science and Engineering: A Multidisciplinary Journal, 13(2), 219-232. 10.1504/IJCSE.2016.078929.
Kumar, P., and S. Gupta (2015). Method for identifying malicious code executions in the cloud based on the order of system calls. Communications., 81, 405425. Wireless Personal. 10.1007/s11277-014-2136-X.
A. Somayaji, S. Forrest, and S. Hofmeyr (1998). System call sequences for detecting intrusions. 6(151–180)Journal of Computer Security. 10.3233/JCS-980109.
Applications, N. Barolli, F. Moscato, T. Enokido, M. Takizawa, and U. Vil- lano. Artificial Intelligence. 2020.DRAFT This is a draft of a paper that will appear in Web, 2L-ZED-IDS: A two-level anomaly detector for numerous attack classes, (n.d.).
Jebamalar, J. P. A., S. Paul, and D. P. P. Latha (1882) are cited as the authority. An in-depth look at how to categorize mined data. Singapore: Springer, 2010. 1007.1007/978-981-13-1882-5.
(2017a) L. Jia, M. Zhu, and B. Tu.Cloud Computing, 10.1109/CCGRID.2017.48, Trustworthy Virtual Machine Introspection (T-VMI)

Jung, J., and H. Zarrabi, 2017.HIDCC is a hybrid method for detecting intrusions in the cloud. 10.1002/cpe.4171.
According to Khalil (I.M.), Khreishah (A.), and Azeem (M.) (2014).Security in the cloud: a literature review, 1–35, 10.3390/computers3010001..
(2017), by Khammassi, C. and Krichen, S. Selecting features for network intrusion detection using a GA-LR wrapper. 70, pp. 255-277 in Computer Security. 10.1016/j.cose.2017.06.005.
M. A. Khan. 2016. An analysis of the current state of cloud computing security. Published in Journal of Network and Computer Applications, DOI: 10.1016/j.jnca.2016.05.010. Pages 11–29.
This year's citations are: Khraisat, A., Gondal, I., Vamplew, P., and Kamruzzaman, J. Methods, data, and difficulties in intrusion detection systems: a review. doi:10.1186/s42400-019-0038-7. Cybersecurit. 2.
It was published in 2014 by Kirat, D., G. Vigna, C. Kruegel, and G. Vigna.Sec14-paper-kirat.Pdf.
In 2009, researchers Bailey, J., Turner, M., Bailey, J., Linkman, S., and Kitchenham, B. A survey of the literature on systematic reviews in software engineering. Research in Computer Software, 51, 7-15, 10.1016/j.infsof.2008.09.009.
P. Kumar, V. S. Nitin, K. Shah, S. S. P. Shukla, and D. S. Chauhan 2011. A new method for protecting data on the cloud, employing a hidden Markov model and clustering. Referenced in WICT 2011 World Congress Proceedings, pages 810–815. 10.1109/WICT.2011.6141351.
2018 S. Laurén.A cloud-based monitoring system for virtual machines, p. 104–109.
T. K. Lengyel, S. Maresca, B. D. Payne, G. D. Webster, S. Vogl, and A. Kiayias published their findings in 2014. The DRAKVUF dynamic malware analysis system is scalable, accurate, and covert. pp. 386–395), 2014–Dec. Proceedings of the Association for Computing Machinery. 10.1145/2664243.2664252.
Research by Lin, C. H., Tien, C. W., and Pao, H. K. (2012). A very effective and efficient NIDS for use in a cloud virtualization setting. Cloud Computing Technology: 4th IEEE International Conference Proceedings. 10.1109/CloudCom.2012.6427583.
Authors: Lo, C. C.; Huang, C. C.; and Ku, J. (2010). A framework for collaborative intrusion detection in cloud computing networks. pp. 280-284 in Parallel Processing: Work in Progress: Proceedings of the International Conference. 10.1109/ICPPW.2010.46.

C. Maiero & M. Miculan 2011. Call-trace-based, stealthy intrusion detection in paravirtualized environments. pp. 300-306). This was published in the proceedings of a conference on cryptography, privacy, and security. 10.5220/0003521003000306.
A. Mukhopadhyay, M. K. Sanyal, P. P. Sarkar, and J. K. Mandal (2015).
Second international conference on information systems design and intelligent applications, India, 2015. Proceedings. Volume 1. Advances in Intelligent Systems and Computing. 339. 10.1007/978-81-322-2250-7.
In L. Marinos & J.M.A survey of recent and future cyber threats: the ENISA danger environment in 2013, 10.2788/14231.
(2014). Meng, Y., Li, W., & Kwok, L. F. Modeling intrusion detection with exclusive signature matching in parallel on the cloud. pp. 175–182) of the IEEE's high performance computing and communications proceedings. 2013 IEEE International Conference on Embeded and Ubiquitous Computing (HPCC 2013), EUC 2013. 10.1109/HPCC.and.EUC.2013.34.