International Journal of Engineering and Management Research e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-2 (April 2023)
https://ijemr.vandanapublications.com https://doi.org/10.31033/ijemr.13.2.35

A Review on Intrusion Detection in Cloud Computing

Monis Tariq[1] and Mohd. Suaib[2]
[1]PG, Department of Computer Science and Engineering, Integral University, Lucknow, INDIA
[2]Associate Professor, Department of Computer Science and Engineering, Integral University, Lucknow, INDIA

[1]Corresponding Author: monistariq3@gmail.com

Received: 28-03-2023 **Revised:** 16-04-2023 **Accepted:** 29-04-2023

ABSTRACT

Rapid growth of resources and escalating cost of infrastructure is leading organizations to adopt cloud computing. Cloud computing provides high performance, efficient utilization, and on-demand availability of resources. We propose an intrusion detection system which is based on the cloud computing to reduce the risk of intrusion on the cloud networks and cover up the deficiency of already in use intrusion detection systems. Intrusion Detection System (IDS) in Cloud Computing is a security solution designed to detect and prevent unauthorized access and malicious activity in cloud computing environments. Cloud computing refers to the use of remote servers hosted on the internet to store, manage, and process data instead of using local servers or personal computers .Our design is based on cloud computing Software-as-a service (SaaS) model for detection and prevention of intrusion cloud-based users. Additionally, the study will also address virtual machine introspection (VMI) and hypervisor introspection (HVI) strategies. The current study is organized on the basis of three distinct: cloud security concerns, the importance of feature selection, and the analysis of existing IDS techniques. Finally, this work presents a review of existing security issues/challenges and research gaps for future research. Then, a combined survey of IDS on the basis of signature and anomaly detection approaches is given in another tabular form so as to get a clear analysis about attacks to be detected, advantages and challenges to be faced by existing methods.

***Keywords*—** Cloud based IDS, Intrusion, Anomaly, Soft Computing

I. INTRODUCTION

Cloud computing is an emerging technology adopted by organizations of all scale due to its low-cost and pay-as-you-go structure. It has revolutionized the IT world with its unique and ubiquitous capabilities. Organization prefers cloud as it replaces the high price infrastructure and need of maintenance. It offers three service models of software as a service (e.g. Google Apps [1]), platform as a service (e.g. Google App Engine Microsoft's Azure and infrastructure as a service (e.g. Amazon Web Service, Eucalyptus , Open Nebula [. Virtualization enables cloud to provide elasticity, ease of use, scalability and on-demand network access to a shared pool of configurable computing resources [2]. Cloud computing paradigm has a service-oriented architecture which has led to a drastic alteration on how services are provided and managed. It is three-tier architecture consisting of infrastructure, platform and applications as a service where each tier is vulnerable and prone to security risks. Attackers can even compromise the integrity, confidentiality and availability of the resources, data and virtualized infrastructure of cloud computing system which may give birth to new types of attacks. The problem can be worse and more critical when a cloud with massive storage capacity and computing power is attacked by attackers present in the cloud itself. Additionally, the use of hypervisors and virtual machines in cloud also create security threats like DDoS attack as they are vulnerable to virtual machine level attacks or hypervisor attacks at IaaS level . In 2017, Equifax U.S. based consumer credit reporting agency became victim of cyber-attack when arose the problem of identity theft for 145.5 million U.S. consumers. The hackers stolen the personally identifiable information including names, social security number, and birth dates etc. of consumers and left no evidence of this unauthorized activity. This was considered to be one of major breach happened in history, costing the company $275 million of loss. Therefore, in today era of hackers, it becomes very crucial to design the system much stronger so as to protect the resources, infrastructure and valuable data from them. Here, Intrusion Detection System plays a significant role in securing customers data, resource assets in cloud computing against security threats. It is one of the advanced security solutions capable of protecting network data from malicious activities. It should be well designed and compatible with the properties of cloud computing also since cloud computing is different from traditional computer systems. It must also be able to detect cloud specific attacks efficiently.

The main focus of this paper is to thorough review of IDS on the basis of its detection techniques in cloud computing environment[2]. This paper is organized as follows: In Section 2, background of IDS in cloud computing is presented. In Section 3 and 4, types of cloud-based IDS and different approaches of detection are

discussed respectively. Then, thorough survey of literature on cloud IDS is given in section 5. In last section, conclusion is followed by references to be referred in throughout the paper[3].

II. BACKGROUND

Intrusion Detection System is an essential component of security measures for protecting computer systems and network against suspicious activities. It is a hardware device or software application that monitors network traffic, system or host activities for policy violations or malicious activity in the system . It issues warning alarm and sends reports to system administrator if such an activity is discovered. However, the warning alerts generated by IDS may be a false alarm or irrelevant to actual intrusion also which affects the performance of the system. IDS have to be designed in such a way that it can also detect false alarm along with intrusions. Furthermore, IDS is expanded to prevention system that can stop or prevent attackers from performing malicious activities after detecting intrusions. It can prevent attacks by changing either configuration of system such as reconfiguring network device to block access of attacker or content of attacked portion or security environment in which attack occurred etc. IDS can also be used in distributed cloud environment to detect cloud specific attacks by deploying it onto cloud devices or VM devices. Because of high false alarm rate generated by IDS, its prevention system can incorrectly identify legitimate normal activity as malicious and can respond inaccurately for that detected activity in cloud computing. Therefore, IDS and IDPS should be designed and deployed such that it can uncover all cloud related attacks over entire cloud network with minimum false alarm rate as possible.

III. TYPES OF CLOUD BASED IDS

Intrusion detection system evolved with the concept of Computer Security Threat Monitoring and Surveillance. It is a proactive technology for monitoring and defensive purpose to protect critical IT infrastructure from suspicious activities. Because of high volume of data and increased complexity of system attacks, usage of IDS has been dramatically raised. Since majority of business, IT sectors are moving towards decentralized architecture such as cloud computing, traditional IDS approach is not adhering to cloud requirements. Thus, the IDS must be distributed in nature to work with cloud networks; it must monitor each and every node in computing environment. IDS in Cloud Computing involve monitoring network traffic, system logs, and other relevant data to identify potential security threats. Some common types of IDS used in Cloud Computing include therefore, considering both traditional and distributed based IDSs, it can be categorized into three kinds as follows[2][3].

Signature-based IDS: This type of IDS identifies known patterns of malicious activity by comparing network traffic against a database of known signatures. These signatures are created by security experts to represent the behavior of known attack

Anomaly-based IDS: This type of IDS identifies abnormal patterns of network traffic that do not match known signatures. These anomalies may indicate potential security threats, such as unauthorized access attempts or data exfiltration. Behavior-based IDS: This type of IDS identifies unusual behavior of users or applications that may indicate a security breach. This approach involves monitoring system logs, user activities, and other relevant data to identify patterns of suspicious behavior[4].

Network based Intrusion Detection System: Network intrusion detection system monitors and analyzes network traffic by reading individual packets through network layer and transport layer. It searches for any suspicious activity or network based attack such as Denial of Service (DoS) attack, port scans etc. Once an abnormal behavior in network traffic is identified, alert can be sent to system administrator. Most of the commercial IDSs are based on the NIDS such as Snort, Tcpdump and Natural flight Recorder (Mehmood, Habiba, et al., 2013). These are well known for general sized networks and convenient for implementation to detect intrusions. However, (Kumar, & Hanumanthappa, 2012) discussed the main issues of Snort IDS when integrating with distributed computing environment. To overcome the issues, they introduced new approach for handling these issues. For virtual network systems, multi phase distributed vulnerability detection and measurement technique has been proposed to detect DDoS attack (Chung, Khatkar, et al. 2013). It has detected attacks based on attack graph by analyzing network traffic flowing through virtual machines. It has significantly improved attack detection and mitigates attack consequences.

Host based Intrusion Detection System: Host based intrusion detection system monitors the individual host or device on the network by analyzing any change in the activity performed by host and events occurring within that host. It looks at every activity of host by checking application logs, system calls, and file-system modifications, inbound and outbound packets to and from host. If any suspicious activity is found, an alert is generated and sent to administrator to protect the system from malicious attack. Since majority of sectors prefer HIDS also after NIDS which are mainly based on the log file analysis of system. A model of HIDS has been developed based on log file analysis of Microsoft Windows XP operating system. It detects intrusions by matching predefined pattern with the logs of operating system [5]

Distributed based Intrusion Detection System: Distributed IDS (DIDS) also known as hybrid IDS, consists of two or more detection methods or systems i.e., NIDS,

HIDS etc. This type of system is deployed over large distributed network like cloud computing so as all entities can communicate with each other and with network monitor such as central server (Premathilaka, 2013). In this way, all hosts deployed over network collect system information and send it to central server by converting it into standard format[6].

Hypervisor based Intrusion Detection System: Hypervisor or Virtual Machine Manager (VMM) is software or hardware, creates and executes virtual machines available over cloud network. It manages each instance of virtual machine. However, virtual machines are also attractive target of potential intruders which makes realization for protecting the virtual machines itself. Thus, for protection of virtual machines and hypervisor itself, hypervisor based IDS are employed over virtual network. It provides abstract layer between virtual machine and underlying host. Hypervisor based IDS is placed inside the hypervisor which detects anomalous actions of users by analyzing the available information over network [8]. It monitors and analyzes the communication between VMs, hypervisors and VM.

IV. DIFFERENT APPROACHES FOR DETECTING AN INTRUSION

In cloud computing environment, only network based or host based intrusion detection system cannot be successful in achieving specified level of security because of distributed computing network. To achieve required performance, intrusions can be detected through different techniques such as signature based, anomaly based or combination of both techniques. However, to increase the efficiency of anomaly based approach, it can be integrated with soft computing techniques like fuzzy logic, artificial neural networks, support vector machines, genetic algorithms etc.

There are several approaches for detecting an intrusion in a computer system. Here are some of the most common Signature or Knowledge Based Intrusion Detection approach: This approach involves comparing the network traffic or system logs against a database of known attack signatures. If a match is found, an alert is generated. Signature-based detection is effective against known attacks but may not detect new or unknown attacks. It refers to the detection of intrusion by matching the specific patterns known as signatures with the patterns available for known attacks .If the pattern gets matched, the alarm will be triggered to warn the administrator. This approach is good for finding known attacks only but not for unknown attacks because it can match the patterns with the stored patterns only.

Anomaly or Behavior Based Intrusion Detection approach: This approach involves creating a baseline of normal system behavior and then monitoring the system for deviations from that baseline. If a deviation is detected, an alert is generated. Anomaly-based detection is effective against unknown attacks but may generate false positives if normal behavior changes over time. Anomaly based IDS are primarily introduced for finding unknown attacks. It identifies the anomalous behavior rather than signatures or patterns based on the examination of data taken from normal usage and checks it against normal behavior. If it deviates from normal behavior pattern, alarm is issued to inform the administrator about intrusion occurred in the system. Besides, it may suffer from false positives, in which it may consider the unknown legitimate activity as malicious activity.

Behavior-based detection: This approach involves analyzing the behavior of users and systems to identify suspicious activity that may indicate an attack. This can include monitoring login attempts, file accesses, and network traffic patterns. Behavior-based detection is effective at detecting insider threats and targeted attacks but may be less effective against automated attacks

Heuristic-based detection: This approach involves using rules and algorithms to identify suspicious activity based on characteristics of known attacks. Heuristic-based detection is effective at detecting unknown attacks, but it may also generate false positives and requires frequent updates to stay effective

Machine Learning-based Detection

This approach involves using machine learning algorithms to identify patterns of suspicious activity in system logs and network traffic. Machine learning-based detection is effective at detecting unknown attacks, can reduce false positives, and can adapt to changing attack patterns over time

Hybrid based Intrusion Detection approach: This approach is a combination of signature and anomaly based detection techniques so that intrusions can be detected in less time and detection system can perform better than individual approaches. A hybrid approach takes advantages of both approaches i.e., detects both known and unknown attacks based on misuse and anomaly methods respectively. In other words, it may be a combination of different soft computing techniques also to detect any type of attack at same instance. In (Desai, & Gaikwad, 2016), authors have combined fuzzy genetic algorithm and signature-based methods to identify external attacks and internal attacks respectively[8].

A combination of these approaches may be used to provide comprehensive intrusion detection and prevention capabilities. It is also important to regularly update and maintain intrusion detection systems to ensure they are effective against new and emerging threats[9].

V. REVIEW OF LITERATURE: CURRENT STATE OF THE ART

In this section, concise overview of what has been studied, argued, and established about cloud-based IDS is discussed. Literature survey is organized thematically based upon the different approaches used for IDS and divided into three subsections. First sub-section deals with related work of IDS on the basis of soft computing methods including machine learning approaches, neural network-based techniques and fuzzy methods. Similarly, second sub-section surveys different methods of data mining and last sub-section contains related work of methods other than these. Every sub-section is ended with containing research findings in tabular form. At the end of this section, combined table of entire survey on the basis of detection approach is given

Based on Soft Computing Approaches used for cloud IDS

In this subsection of the paper, research findings are organized in terms of soft computing methods or algorithms implemented for the intrusion detection process in cloud computing. Various types of this approach have been used by different researchers. Soft computing, sometimes referred as computational intelligence, is used for solving difficult tasks such as NP-complete problems. Intrusion detection is one of NP-complete problem which cannot be solved in polynomial time. The main constituents of soft computing considered in this paper are machine learning, artificial neural network and fuzzy logic approaches [11]. Table 1 provides a comprehensive study of proposed cloud IDS based on these three approaches.

References	Algorithm Preferred	Description
Kozik et al., 2018	Extreme Learning Machine	It has detected anomaly based attacks such as DoS by distributing traffic classification over edge devices using the concept of machine learning approach.
Idhammad et al., 2018	Random Forest and Naive Bayes Classifiers	It has proposed methodology to detect anomaly based intrusions in five modules using machine learning classifiers. It has used CIDDS-001 dataset to compare its results with other methods.
Gill, & Buyya, 2018	Support Vector Machine (SVM)	This paper mainly focussed on secure resource management aspect of cloud. It has proposed self- protected approach against attacks. It has also analyzed impact of Quality of Service along with the availability of services for authorized users.
Aljawarneh et al., 2018	Machine learning based hybrid classifiers	It has proposed hybrid model for anomaly based intrusion detection based on threshold degree of network transaction's data. It has significantly reduced the computational and time complexity.
Alzahrani, & Hong, 2018	Back Propagation Neural Networks	It has proposed hybrid model for detecting both kinds of signature based and anomaly based intrusions. It has used the concept of artificial neural network approach to detect attacks such as DDoS.
Modi et al., 2016	Snort for signature based detection and Back Propagation neural network for anomaly based detection	In this paper, known and unknown attacks such as DDoS and DoS etc. are detected using hybrid network intrusion detection system over cloud. It has improved overall detection rate and achieved results within very less detection time.
Alfy, & Al-Obeidat, 2014	Fuzzy Classification method	This paper has detected intrusions based on anomalies in the traffic. It dealt with various kinds of attributes using greedy selection approach and then detected attacks.
Xiong et al., 2014	Synergetic neural network approach	In this research work, it has analyzed network traffic of cloud based on its dynamic characteristics. However, it has not detected any specific type of attack but considered all attacks as anomalies.

Table 1: Summary of intrusion detection schemes based on soft computing approaches

VI. BASED ON DATA MINING APPROACHES USED FOR CLOUD IDS

Data mining is another approach based on which survey is differentiated. Various data mining approaches have been employed for detecting intrusions from large data sets. First, it extracts the required information from data sets of large size using feature selection approaches. Then, it detects the intrusions from selected information[12]. It involves different clustering and classification approaches through which data is processed. Thus, Table 2 provides extensive study about data mining algorithms being used by many authors so far.

References	Algorithm Preferred	Description
Peng et al., 2018	Mini Batch K-means Clustering approach	This paper has used principal component analysis followed by mini batch clustering method to manage massive data and to improve the efficiency of approach.
Deng et al., 2017	K-means Clustering	This paper mainly focussed on improvement of parameters like detection time and detection rate of cyber physical systems such as smart grid. It has detected attacks using gene expression programming concepts.
Arjuna, & Modi, 2017	Decision tree, random forest classifiers, linear discriminant analysis	It has proposed secure detection system for virtual network layer of cloud. It has combined both signature and anomaly methods, detected evidences of distributed attacks and applied Dempster-Shafer Theory for decision making.
Chen et al., 2016	K-means Clustering and Naive Bayes	In this paper, architecture for network monitoring and threat detection in cloud computing environment has been proposed.
Modi et al. 2012	Signature Apriori Algorithm	The purpose of this research is to find the known attacks and the derivatives of them by monitoring network traffic. However, it has not detected unknown attacks.

Based on Other Methods

The remaining approaches other than soft computing and data mining have been summarized in this sub-section. It may include snort-based algorithm for traffic analyzing, graph-based methods for virtual network systems etc[13]. There are fewer methods other than human inspired and mining algorithms employed for detecting attacks over network. The summarization is given here in below table 3.

References	Algorithm Preferred	Description
Wang et al., 2020	Rabin Fingerprint Algorithm	It has followed novel approach of cloud computing i.e., fog computing in which it has reduced the workload of cloud servers by offloading computational task of detection to the edge devices.
Mahajan, & Peddoju, 2018	Snort	It has used hybrid approach of IDS integrated with honeypot network to mitigate both known and unknown attacks. In addition, it has also analyzed the malware activities to detect the effects of malicious attacks.
Chung et al., 2017	Attack graph approach	To prevent vulnerable virtual machines from attackers, it has proposed multi-phase distributed vulnerability detection approach for virtual machines available over cloud network.
Lo et al., 2016	Snort	To reduce the impact of DoS, DDoS attacks; it has proposed cooperative intrusion detection system. It has in cooperated cooperative agent to compute and determine whether attack has detected or not.

Table 3: Summary of intrusion detection schemes based on other approaches

References	Algorithm Preferred	Description
Wang et al., 2020	Rabin Fingerprint Algorithm	It has followed novel approach of cloud computing i.e., fog computing in which it has reduced the workload of cloud servers by offloading computational task of detection to the edge devices.
Mahajan,& Peddoju, 2018	Snort	It has used hybrid approach of IDS integrated with honeypot network to mitigate both known and unknown attacks. In addition, it has also analyzed the malware activities to detect the effects of malicious attacks.
Chung et al., 2017	Attack graph approach	To prevent vulnerable virtual machines from attackers, it has proposed multi-phase distributed vulnerability detection approach for virtual machines available over cloud network.
Lo et al., 2016	Snort	To reduce the impact of DoS, DDoS attacks; it has proposed cooperative intrusion detection system. It has in cooperated cooperative agent to compute and determine whether attack has detected or not.

At the end of above sub-sections, combined study is conducted comprehensively based upon the detection approaches such as signature based and anomaly based. Various research findings have been further classified in three sub-sections in table 4. Each sub-section analyzes each technique broadly mainly on the basis of IDS type (either NIDS or HIDS or DIDS), cloud service delivery layer, type of attack detected, its advantages and challenges faced by researchers[14,15]

IDS approach	Year	IDS type	Cloud layer	Attack detected	Advantages	Disadvantages
	2018	DIDS	IaaS	---	Proposed a privacy preserving framework for distributed environment using the concept of fog computing.	It has not detected any type of attack.
	2017	NIDS	---	SQL injection, malware injection, XSS* attack, SSH†	It has used integrated approach of IDS with honeypot network to trap the intrusions.	DoS attacks cannot be detected.
	2014	NIDS	---	IP spoofing	Evaluated the performance using different data sets including real data set.	Not implemented for wireless and distributed environments.
Signature						
	2013	NIDS	IaaS	DDoS	Detected attack over virtual network environment.	To cover entire spectrum of IDS solutions, host based IDS needed to be incorporated.
	2012	NIDS	IaaS	DoS, DDoS	Detected known attacks and derivatives of known attacks	It has not detected unknown attacks. Only theoretical analysis is done.
	2011	NIDS	SaaS	DDoS	Cost of classification error has been minimized.	Only known attacks could be detected.
	2010	DIDS	---	DoS	It keeps IDS from single point of failure.	Increases computation effort as compared to Snort.

	2010	NIDS	IaaS	DoS	It secures multiple virtual machines from DoS attacks.	It could not detect unknown attacks.
	2018	NIDS	IaaS	DoS	Deep traffic inspection and classification done over edge devices.	Only Single detected. Type of attack
Anomaly	2018	NIDS	SaaS	DoS, Probe, U2R‡, R2L§	Detected multiple attacks with good accuracy rate.	Although detected many attacks but unable to detect DDoS attack because of centralized environment.
	2016	NIDS	IaaS	DDoS, Port Scanning	Suitable for real time scenarios.	It has taken heavy software. It has not detected other types of attacks.
	2015	NIDS	---	Probe, DoS, U2R, R2L	Experimental results are shown very well.	Not implemented over real time databases.
	2014	NIDS	---	DoS, U2R, R2L, Probing	It has given better results using greedy selection approach prior to classification method[16]	It has not implemented for real time scenario.
	2014	NIDS	---	---	Detected network traffic dynamic characteristics based using different approaches. on two	It has not detected specific type of attack. Considered all attacks as anomalies.
	2011	HIDS	---	U2R, R2L	It requires less system resources and it can be computed in real time.	This approach works over Windows operating system only.
	2018	NIDS	SaaS	DDoS, Probe, DoS, U2R, R2L	Detected several attacks and analyzed the impact of security on QoS.	No practical implementation over real cloud environment.
Signature and Anomaly	2018	NIDS	---	DDoS	Performed experiments on real time public cloud.	It has not compared its results with other existing approaches.
	2017	NIDS	---	DDoS	Compared results very well using different approaches.	It is suitable for virtual networks only.
	2016	DIDS	SaaS	SQL Injection, R2L	This hybrid system can work in offline as well as online environment.	Not implemented for distributed environment.
	2016	NIDS	IaaS	DoS, DDoS	It has detected internal as well as external attacks with low computational Cost[17].	Not given any experimental results.

VII. CONCLUSION

Intrusion Detection System is enacted in enhancing the cloud security. It helps in achieving confidentiality, integrity and availability (CIA) of data and network in cloud computing. Various intrusion detection approaches have been employed to detect security attacks evolved over cloud network. The paper emphasizes over existing methods of IDS based on soft computing techniques, data mining and other approaches. Then, the entire survey is categorized based on detection approaches such as signature and anomaly to get vivid analysis about type of attack to be detected, advantage of using the approach, loopholes existed in implementing approach in a tabular manner. As per the survey conducted, anomaly based detection approach is adopted by many researchers to detect both known and unknown attacks by monitoring network traffic.

REFERENCES

[1] Iqbal, S., Kiah, L.M., Dhaghighi, B., Hussain, M., Khan, S., Khan, M.K. & Choo, K.R. (2016). On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. *International Journal of Network and Computer Applications, 74*, 98-120.

[2] Wasim Khan, M. H. (2022). An unsupervised deep learning ensemble model for anomaly detection in static attributed social networks. *International Journal of Cognitive Computing in Engineering*, 153-160.

[3] Khan, W. & Haroon, M. (2022). An efficient framework for anomaly detection in attributed social networks. *Int. J. Inf. Tecnol., 14*, 3069–3076.

[4] Patel, A., Taghavi, M., Bakhtiyari, K. & Junior, J.C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of Network and Computer Applications, 36* (1), 25-41.

[5] Husain, Mohammad Salman & Haroon, Dr. Mohammad. (2020). An enriched information security framework from various attacks in the IoT. *International Journal of Innovative Research in Computer Science & Technology (IJIRCST), 8*(3). Available at: SSRN: https://ssrn.com/abstract=3672418.

[6] Zeeshan Ali Siddiqui & Mohd. Haroon. (2023). Research on significant factors affecting adoption of blockchain technology for enterprise distributed applications based on integrated MCDM FCEM-MULTIMOORA-FG method. *Engineering Applications of Artificial Intelligence, 118*, 105699. DOI: 10.1016/j.engappai.2022.105699.

[7] Kumar, M., Hanumanthappa, M. & Kumar, T.V.S. (2012). Intrusion detection system using grid computing using Snort. *International Conference on Computing, Communication and Applications*, 1-6.

[8] Husain, Mohammad Salman. (2020). A review of information security from consumer's perspective especially in online transactions. *International Journal of Engineering and Management Research, 10*(4). Available at: SSRN: https://ssrn.com/abstract=3669577

[9] Zeeshan Ali Siddiqui & Mohd Haroon. (2022). Application of artificial intelligence and machine learning in blockchain technology, Artificial Intelligence and Machine Learning for EDGE Computing. *Academic Press*, pp. 169-185. https://doi.org/10.1016/B978-0-12-824054-0.00001-0.

[10] Afsarudfin and Pratiksha and Haroon, Mohd & Ahamad Faiyaz. (2021). Satiating a user-delineated time constraints while scheduling workflow in cloud environments. *International Journal of Innovative Research in Computer Science& Technology (IJIRCST)*. Available at: SSRN: https://ssrn.com/abstract=3880002.

[11] Kene, S.G. & Theng, D.P. (2015). A review on intrusion detection techniques for cloud computing and security challenges. *IEEE Sponsored 2nd International Conference on Electronics and Communication Systems*, pp. 227-232.

[12] Liao, H. J., Lin, C. H. R., Lin, Y.C. & Tung, K.Y. (2013). Intrusion detection system: A comprehensive, *Journal of Network and Computer Applications, 36*, 16-24.

[13] Desai, A.S. & Gaikwad, D.P. (2016). Real time hybrid intrusion detection system using signature matching algorithm and fuzzy-GA. *IEEE International Conference on Advances in Electronics, Communication and Computer Technology*, pp. 291-294.

[14] Ibrahim, D. (2016). An overview of soft computing. *12th International Conference on Application of Fuzzy Systems and Soft Computing*, pp. 34-38.

[15] Kozik, R., Choras, M., Ficco, M. & Palmieri, F. (2018). A scalable distributed machine learning approach for attack detection in edge computing environments. *Journal of Parallel and Distributed Computing, 119*, 18-26.

[16] Idhammad, M., Afdel, K. & Belouch, M. (2018). Distributed intrusion detection system for cloud

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-2 (April 2023)
https://doi.org/10.31033/ijemr.13.2.35

environments based on data mining techniques. The First International Conference on Intelligent Computing in Data Sciences, 35-41.

[17] Gill, S.S. & Buyya, R. (2018). SECURE: Self-protection approach in cloud resource management. *Journal of IEEE Cloud Computing, 5*(1), 60-72.

[18] Alzahrani, S. & Hong, L. (2018). Detection of distributed denial of service (DDoS) attacks using artificial intelligence on cloud. *IEEE World Congress on Services*, pp. 35-36.

[19] [17] Chiba, Z., Abghour, N., Moussaid, K., Omri, A. E. & Rida, M. (2016). *A cooperative and hybrid network intrusion detection framework in cloud computing based on snort and optimized*.