Enhancing Cloud Security: An In-Depth Analysis Of Intrusion Detection And Prevention Systems

Sangeeta Joshi

(Assistant Professor, Mata Gujri College, Fatehgarh Sahib)

Abstract: Nowadays, Due to the rapid growth of distributed systems, IT organizations are inclining towards the cloud computing environment. The intercommunication between distributed systems widens the possibility of confrontation against cyber attackers or intruders. The technology for accumulating and preserving the user's information at an affordable cost and refined services is known as cloud computing. The emergence of cloud computing and its deployment all over the world necessitates security through intrusion detection and prevention system (IDPS). Intrusion Detection and Prevention System plays an efficient role in differentiating the usual and unusual behavior by the verification, supervision, control of the log files and configuration, user activities, network traffic, etc. The present communication highlights the existing approaches of known (Signature based), unknown (Anomaly based) attack detection, and hybrid approaches that are mandated to overcome the security challenges in an ongoing time. Moreover, the disclosure in terms of comparative analysis of utilized techniques is also presented. The novelty of this work incorporates the comparison of diverse approaches utilized for the identification and prevention of attacks in the cloud environment. It also covers existing datasets along with research gaps in the existing approaches.

Keywords: Anomaly Based, Cloud Computing, Intrusion Detection System, Intrusion Prevention System, IDPS, Signature Based.

Introduction: Cloud computing is the branch of information and communication technology (ICT) that administers virtual resources such as networks, storage, servers, and applications to the users on-demand and pay-per-use basis (Hatef et al., 2018). The NIST i.e., National Institute of Standards and Technology proposes cloud computing by taking into consideration five foremost characteristics such as bandwidth, measured services, rapid flexibility, on-demand service, and resource pooling. It further comprises three service delivery models particularly software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS) (Mell & Grance, 2011). (Shamshirband et al., 2020) also proffered the pros and cons of all the delivery models from which security is a major concern.

One of the most significant assets of all organizations is the vast quantity of sensitive information stored in the public cloud. The information is vulnerable to security hazards such as availability, confidentiality, and integrity of the organization (Thilagam & Aruna, 2021). Though, reliability and convenience are the main reasons for using a cloud computing environment. Beyond, these uninterrupted services of the cloud environment, it attracts the attackers to gain access and exploit services provided by the service provider. Attack in the cloud environment

affects the end user's confidential data, bandwidth usage, cloud resources, etc. These resources and services can be protected from malicious activities using the firewall, Intrusion Detection System, and Intrusion Prevention System. A firewall can recognize only insider attacks and is not able to detect outsider attacks such as Distributed Denial of service attacks (DDoS) (Pandeeswari & Kumar, 2016). To defend the cloud environment from suspicious activities a hybrid approach to Intrusion detection and prevention system (IDPS) is required. The Intrusion detection and prevention system is essentially employed to monitor the network, collect, analyze the information, identify the behavior of the packets, and prevent attacks in the cloud environment.

There exist two phases for intrusion detection such as known attack detection (Signature-based or misuse-based) and Unknown attack detection (Anomaly-based) phase. The known-attack detection phase is the knowledge-based detection system used to determine the incoming attacks in the cloud by matching patterns with the predefined signature stored in the database.

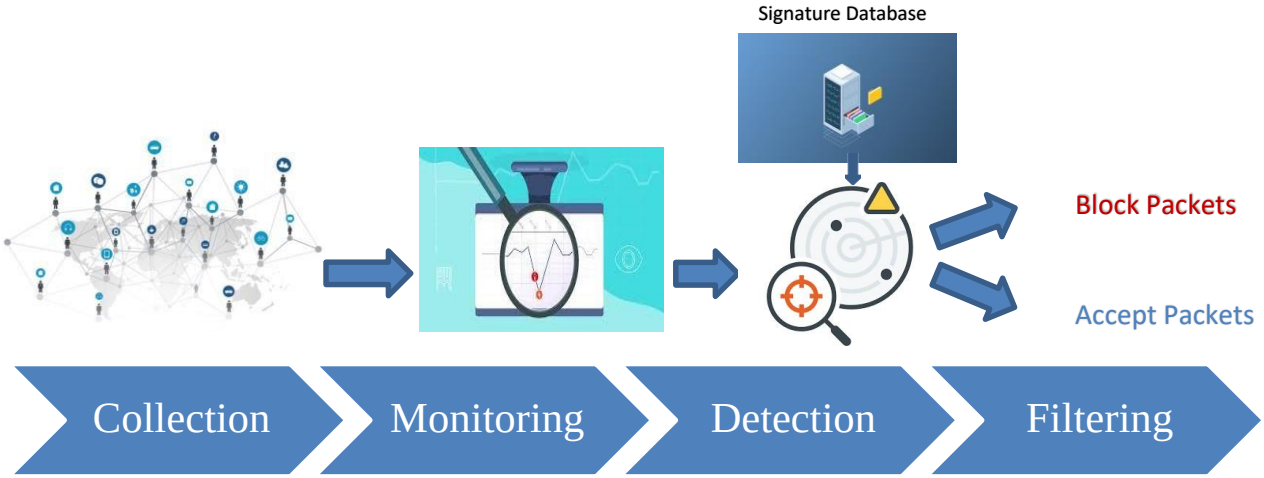

Figure 1: Basic work flow of Attack Detection

The known attack detection phase consists of four phases as shown in Figure 1 (Snehi et al., 2020). Another technique, the unknown-attack detection is the behavior-based detection system used to identify the behavior of the packets. If the behavior detected is abnormal, it is considered an anomaly or unknown attacks (Hatef et al., 2018). Thus, this technique can detect novel or unknown attacks. If any normal behavior is wrongly identified as an attack in the network is considered as a false positive. And if the system considers abnormal behavior as normal is treated as false negative. The known attacks detection phase has higher accuracy compared to the unknown attack detection phase (Ghosh et al., 2016). The purpose of the Hybrid approach i.e., the combination of known and unknown attack detection phase is to detect internal as well as external attacks, minimizing computational cost, enhancing accuracy, reducing false alarms, etc. This approach combines the benefits of known attack detection phase with its detection speed and unknown attack detection phase with the possibility to detect novel attacks.

Motivation and contributions:

Cloud computing is constantly growing. Its nature is to empower the processing task in the cloud environment. Security in cloud computing has received wide attention from the scientific community. However, a comprehensive investigation of various techniques of IDPS is still lacking. Thus, filling this gap is the inducement of research.

Table 1 emphasizes the novelty of our profound analysis. This research depicts the comparison of present and previous related work. The article first provides an insight about cloud computing, then it provides a comprehensive analysis of Known attack detection (Signature-based detection), Unknown attack detection (Anomaly based detection), and Hybrid approach based on its detection and prevention techniques in a cloud computing environment. The presented research tries to overcome the security challenges and issues with the cloud network. It also covers the advantages and drawbacks of the existing approaches for known attacks shown in Table 1 and unknown attacks represented in Table 2.

Ref	Signature Based IDS Overview	Anomaly Based IDS Overview	Hybrid Approach to IDPS	Open Issues
(Modi et al., 2012)	✓	✓		
(Sengaphay et al., 2016)	✓			
(Mishra et al., 2016)	✓			✓
(Chiba et al., 2016)	✓	✓	✓	✓
(Gaddam & Nandhini, 2017)	✓	✓		✓
(Bada et al., 2020)	✓			
(Alam et al., n.d.)	✓	✓	✓	
(Alturfi et al., 2021)	✓	✓	✓	
This Paper	✓	✓	✓	✓

Table 1 – Comparison of the present work with the literature

The following considerations are given for the contribution of research work:

1. It includes an overview of cloud computing with intrusion detection and prevention system including diverse approaches for attack detection.
2. The different techniques used for Signature-based detection, Anomaly-based detection, and hybrid approaches are described.
3. Furthermore, it provides the description of different open-source tools for the detection of signature-based attacks in the cloud environment and also depicts which tool generates better results.
4. The research work also provides a brief overview of several datasets available for IDS.
5. Finally, this paper comprises future perspectives for the detection of attacks in the cloud environment.

Other sections are framed as follows: Section 2 exhibits the research methodology employed to accomplish this survey. Section 3 describes the prior work on IDPS. Section 4 identifies several research gaps in the known attack detection phase, unknown attack detection phase, and hybrid approach, and the last section covers the conclusion to be followed by references referred to in the paper with future recommendations.

2. **Research Methodology**: This section covers the research methodology for the paper selection to present the survey of the work done in the given area. A systematic approach has been applied for conducting this research. Figure 2 indicates the approach employed in this research.

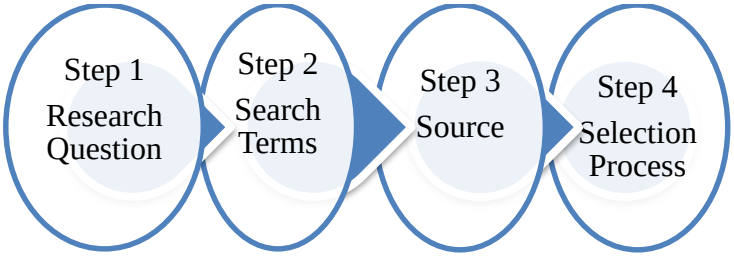

Figure 2: Steps for Research work

2.1 Research Question: Table 2 covers the research questions and also exhibits the reason for each question.

Table 2 – Research Questions

Sr No.	Question	Reason
1.	What are the different techniques used for Known attack detection, Unknown attack detection, and the hybrid approach?	It identifies the different techniques for the detection and prevention of attacks in the cloud environment
2.	What are the different open-source tools for detection and prevention of attacks in cloud environment?	For the detection of Signature-based intrusion attacks in cloud.
3.	Which open-source IDPS is better in detecting specific network attacks?	It exhibits which tool is best for identifying the attacks in the cloud environment.
4.	What are the different parameters that need to be considered for comparing the existing approaches of known attack detection, unknown attack detection, and hybrid approach?	This part covers the comparison of the existing techniques using different performance parameters such as Accuracy, FAR, Detection rate, etc.

2.2. Search Terms: The research work comprises of conducting a comprehensive analysis on diverse approaches of intrusion detection and prevention in the cloud computing environment. Initially, the review articles are searched using the following strings:

- Intrusion detection system
- Intrusion prevention system
- Intrusion detection Literature review
- Intrusion detection systematic study
- An intrusion detection system in the cloud
- Signature based intrusion detection
- Signature based intrusion detection using snort tool
- Anomaly based intrusion detection

- A hybrid approach to intrusion detection and prevention in the cloud.

2.3. Sources of Information:

Various databases were explored, to answer the research questions outlined earlier. Most relevant and reputed journals, books, conferences, and, workshop proceedings were studied. Various databases like Science Direct, ACM Digital Library, Springer LNCS, Google Scholar, Inderscience, IEEE explore, Taylor and Francis, etc. were searched.

2.4. Selection Process

The selection process for the presented research is as follows: First and foremost, the research questions are framed, and various databases are explored for the collection of information. The papers are included or excluded based on the following:

1. Title of the paper.
2. Abstract and keywords.
3. Content of the paper.

This research includes papers that have relevant titles, summary, abstract, and complete detail that satisfies the research questions. otherwise, the papers are excluded.

3. Prior work on IDPS:

IDPS plays an efficient role in securing the network from intruders by detecting the intrusion using IDS and taking preventive action using IPS. There exist three phases for attacks detection: Known attack detection phase, Unknown attack detection phase, and Hybrid approach for detecting known and unknown attacks.

3.1. Known/Signature-based Attacks Detection Phase:

Known attacks detection or Signature-based detection describes the set of patterns or rules already stored in the database. This phase entails open-source intrusion detection systems such as Snort, Suricata, and Bro. These tools are used as signature-based intrusion detection that is open-source, free, configurable, and useful tools. These intrusion detection and prevention systems can be executed on distinctive platforms such as Linux, Windows, etc. The system operates by distinguishing the packets emerging from the network and later compare the content with the predefined patterns and signatures (Hatef et al., 2018).

(Bada et al., 2020) depicts the comparative analysis of different open-source IDS that are used for detecting threats in the network. These tools are used to identify normal and malicious attacks in the network. From the observation, it is clear that the detection rate of Snort IDS is 98.50% that is ahead of Bro which has detection rate of 96.40% and Suricata has detection rate of 97.40%.

(Shah & Issac, 2018) examines the working of two open-source intrusion detection systems such as Snort and Suricata. Snort and Suricata were installed on the two computers with identical configurations that symbolizes, Suricata can process the high-speed network traffic with tremendous consumption of computational resources as compared to Snort. From the experiment, the author suggests, the detection rate of Snort is higher and is further

selected for experiments. The Snort resulted in a high false alarm rate and this problem can be resolved by using Snort's adaptive plug-in. The author used a hybrid approach of SVM and fuzzy logic for improving the detection rate. It helps in accurately detecting the malicious or legitimate packets based on rules given by the IDS. The drawback of Snort is the higher packets drop rate due to the speed of the network traffic and, it cannot process all the packets.

(Sengaphay et al., 2016) proposed an approach for detecting behavior in the private cloud using multi- sensors. The author proposed an improved Snort-IDS for detecting the behavior in a private cloud. The private cloud works better because it adjusts the system, memory, resources as per the requirement. To detect the behavior in the private cloud multi-sensors are used and multiple sensors are installed in the cloud that works according to the snort-IDS rules. Each sensor helps in detecting the intrusion behavior and the alert will be sent to the database. The author considered five types of intrusion behavior like Port scanning, IP address, Operating system, Application behavior, virus or malware behavior. The result of the multi- sensor cooperated with the snort-IDS and help in detecting 51 cases of intrusion behaviors.

(Khamphakdee et al., 2014) proposed an improved Snort-based IDS for detecting the network Probe attack. Author used MIT-DARPA 1999 dataset for evaluating the behavior of Snort that includes the normal and abnormal traffic. Initially, the existing Snort-IDS was analyzed to improve the proposed rules and then, the Wireshark was used to analyze the packets in dataset. After the evaluation, the Snort was updated with improved set of rules that show more accurate results. This approach can work only for probe attack and real time traffic. Different categories of attacks are not considered using this approach.

(Beigh & Peer, 2014) provides an aspect of the performance of different IDS implemented on the DARPA 99 dataset. This paper outlines the comparative analysis of the three most popular IDS such as Snort, Suricata, and Bro. From the experiment, it is analyzed that the performance of Snort is better than the other two IDS.
(Alhomoud et al., 2011) analyzed the performance of Snort and Suricata on different platforms such as Linux 2.6, ESXi server, and FreeBSD. This paper aims to analyze the performance of signature-based IDS on a high-speed network. The study concluded that the snort performs better on FreeBSD and Suricata on Linux 2.6 while handling high-speed network traffic.

Table 1 - Summary of intrusion detection and prevention system for Known attack detection phase.

Reference	Approach	Detection Rate	FNR	FPR	Merits	Demerits
(Bada et al., 2020)	Snort	98.5%	7.1%	54.7%	From the observation, it is clear that Snort is superior to the other two open source IDSs.	The system is not able to work in the real network environment and does not process high speed network traffic.
	Suricata	97.40%	11.3%	72.83%		
	Bro	96.40%	8.97%	67.5%		
(Shah & Issac, 2018)	Snort	N/A	6.7%	55.2%	Snort plugin can be created for further experiment, in order to reduce the FPR.	The tools used in this approach considered only limited parameters.
	Suricata	N/A	16.7%	74.3%		
(Sengaphay et al., 2016)	Snort	51%	N/A	N/A	The system helps in identifying different kind of behavior such as port scan, IP address, OS, application, and virus.	Difficult to prepare rules for multiple sensors in a private cloud.
(Khamphakdee et al., 2014)	Snort	100%	N/A	N/A	The system will regularly update the rules. The occurrence of same attack will be quickly analyzed by the system administrator.	This approach can detect only probe network attack and is not able to detect recent attacks such as Dos, U2R, R2L.
(Beigh & Peer, 2014)	Snort	96.95%	N/A	6.8%	Detection rate of Snort is high and FPR is low compared to other open-source IDS.	There exist some other parameters that need to be considered for the selection of IDS.
	Suricata	96.68%	N/A	12%		
	Bro	76.83%	N/A	3.40%		
(Alhomoud et al., 2011)	Snort	99.7%	N/A	N/A	After evaluation, it is concluded that the performance of Snort is better on FreeBSD and Suricata performs better on Linux.	Snort resulted in higher utilization of CPU and maximum packets drop rate in Linux compared to FreeBSD. And Suricata resulted in maximum utilization of CPU and fewer packets drop rate in Linux compared to FreeBSD.
	Suricata	66.8%	N/A	N/A		

N/A -Not Available

The virtue of a known attack detection/ Signature-based detection system is its simplicity and efficiency. From the analysis as shown in Table 1, Snort is superior IDPS, unlike the other two open-source IDPS such as Suricata and Bro. Snort IDPS assists in defending the system from intrusions such as DoS, DDoS, probe, port scan, IP address, etc. The detection rate of Snort is higher and the False positive rate (FPR) is lower compared to Suricata and Bro IDS. The various challenges are identified such as speed, few parameters are considered, incapability of handling extensive volume of traffic, low detection rate for least frequent attacks such as R2L and U2R, etc.

3.2. Unknown/Anomaly-based Attacks Detection Phase:

The second phase entails the comparison of different approaches used for unknown attack detection. This approach is used to identify the behavior of the traffic. It can detect novel attacks or unknown attacks. Different

authors suggested distinct approaches for the detection of behavior in the network.

(Pandeeswari & Kumar, 2016) proposed an anomaly-based intrusion detection system that uses a hybrid algorithm by combining the Fuzzy C-Means clustering algorithm and Artificial Neural Network at the hypervisor layer. The hypervisor detector is implemented at the virtual machine to monitor the activities in the dynamic environment. Cloudsim 3.0 simulator is used for training and testing the hypervisor in a virtual machine. The proposed system was compared with other techniques such as the Naive Bayes classifier and classic ANN algorithm, which resulted in high detection accuracy and low false alarm rate. The Naive Bayes and ANN algorithm yield a lower detection rate for U2R and R2L attacks. Thus, to improve the performance FCM-ANN approach is used. Although, the training time of ANN is much high. The proposed approach achieved high detection accuracy and a low false alarm rate for the least frequent attacks.

(Ghosh et al., 2016) proposed a method for anomaly-based IDS in the cloud environment. The author presented a novel Penalty Reward-based Fuzzy C-Means Clustering (PRFCM) algorithm and a modified approach to KNN based on Dempster Shafer Theory for classification. The rule set is generated by the PRFCM algorithm, and the best rule set is extracted by using the modified approach to KNN. This approach helps in detecting novel attacks as well as variations of existing attacks. The proposed methodology overwhelms the problem of sensitivity to noise. The author recommended extensive security for the cloud environment by implementing an intrusion detection and prevention system (IDPS).

(Raja & Ramaiah, 2017) suggested a hybrid system for intrusion detection by using fuzzy systems that span four different phases. This system comprises the modified k-means clustering algorithm, to improve the computational speed by using Minkowski distance to provide the clusters. The clusters are evaluated by using the type-2 fuzzy logic-based genetic algorithm. Fuzzy neural networks and Genetic algorithms are combined to achieve a competent detection rate for all types of attacks such as more or less frequent attacks. The system resulted in a higher execution time on clustering of the non-linear dataset.

(Balamurugan & Saravanan, 2019) proposed an enhanced intrusion detection and prevention system in the cloud environment. The approach includes hybrid classification and OTS (one-time signature) generation. Two novel algorithms were proposed by the author such as packet scrutinization algorithm and hybrid classification model i.e., NK-RNN (normalized K-means clustering algorithm and recurrent neural network). The approach for preventing the user from the attack is OTS (one-time signature) was proposed for the cloud users to access the data from the cloud environment. The recommended system works efficiently, which was proved experimentally by comparing the results with the existing approaches.

(Jaber & Rehman, 2020) proposed an FCM-SVM (fuzzy c-means clustering and support vector machine) based intrusion detection system for cloud environment. The proposed method consists of three distinct phases for the objective to be achieved. The primary phase divides the dataset into a number of clusters using fuzzy clustering, the secondary phase train and test the clusters with the SVM algorithm and the last phase consists of a fuzzy aggregation module for consolidating the outcome. From the comparative analysis, it is concluded that the hybrid approach of FCM-SVM detects inconsistencies with high accuracy and low false alarm rate than the other techniques.

(Samriya & Kumar, 2020) introduced a hybrid approach by adopting the fuzzy-based ANN, which was further optimized using the spider monkey optimization algorithm. The hybrid approach handles different security issues such as data leakage, fake identity detection, phishing, etc. The fuzzy-based ANN performs the clustering that was further optimized by the spider monkey optimization (SMO) algorithm. This approach automatically modernizes the fitness value instead of iterative classification and selection. The SMO algorithm eliminates the barrier of overfitting by reducing the dimensions of the dataset. The proposed approach resulted in improved accuracy and reduced computational time compared to the existing approaches.

(Singh & Ranga, 2021) proposed an effective network intrusion detection system for anomaly-based detection in the cloud environment. The author proposed an ensemble-based machine learning approach that uses the classifiers such as a Boosted tree, bagged tree, RUSBoosted tree, subspace discriminant. This approach can be implemented using the CloudSim simulator that works on CICIDS 2017 dataset for analyzing the traffic. The dataset is to be processed by applying different operations such as normalization, one-hot-encoding, etc. The approach resulted in increased accuracy with a reduced period.

(Srilatha & Shyam, 2021) proposed an intrusion detection system in the cloud environment by using the combination of kernel-fuzzy c-means and an optimal type-2 fuzzy neural network. These classifiers help in detecting unauthorized threats and allow the storage of only normal data in the cloud. This model consists of two phases: the first phase includes KFCM i.e., kernel fuzzy c-means that generate the clusters of data; the second phase assign each cluster a type-2 fuzzy neural network to categorize the data as normal or intruded. The proposed model gives better results than the existing IDS.

Table 2 - Summary of intrusion detection and prevention system for Unknown attack detection phase.

Reference	Approach	Detection Rate	Accuracy	Dataset	Advantage	Drawbacks
(Pandeeswari & Kumar, 2016)	ANN& FCM	Normal:96% DDOS: 99% Probe: 63% R2L: 81% U2R: 75%	N/A	KDDCup'99	FCM-ANN approach improves the detection rate of least frequent attacks.	This approach isn't enough to manage a huge volume of data.
(Ghosh et al., 2016)	PRFCM +KNN	76.4%	88.3%	NSL-KDD	It improves the limitations of FCM.	The system can only recognize the attack and is not able to prevent it.
(Raja & Ramaiah, 2017)	Type-2 fuzzy neural network and GA	98.59%	DoS:99.8% Probe:96.8% U2R:99.3% R2L:99.1%	CIDS	CPU consumption is less compared to other approaches.	Its speed is slow for the small number of nodes.
(Balamuruga n & Saravanan, 2019)	NK-RNN and OTS	DoS:100% Probe:100% U2R:85% R2L:85%	N/A	Real time traffic	The proposed model detects novel and zero-day attacks.	Detection rate for least frequent attacks is low.
(Jaber & Rehman, 2020)	FCM- SVM	N/A	DDoS:99.1% Probe:98.8% R2L:98.4% U2R: 97.3%	NSL-KDD	The proposed method improves the accuracy of least frequent attacks.	This approach necessitates investigation for achieving overall accuracy.
(Samriya & Kumar, 2020)	FCM- SMO	N/A	86%	NSL-KDD	Reduced Computational time.	Recent attacks and Security issues need to be considered.
(Singh & Ranga, 2021)	Ensemble based machine learning + Voting Algorithm	97% (approx.)	97.24%	CICIDS 2017	The execution time is reduced with the approach.	Computational time is higher.
(Srilatha & Shyam, 2021)	Kernel Fuzzy c-means and optimal type 2 fuzzy neural network.	DoS:99.1% Probe:79.3% U2R:81.6% R2L:87.4%	N/A	NSL-KDD	The system avoids the unauthorized and illegal activities of data coming in cloud.	There exist some other parameters that needs to be considered for the detection and prevention of threats.

N/A -Not Available

The anomaly-based / Unknown attack detection phase works by identifying abnormal or anomaly behavior in the system. The study concluded that different techniques such as ANN, FCM, SVM, etc. are used for identifying unknown behavior in the network. The limitation of FCM-ANN i.e., the low detection rate for least frequent attacks is overwhelmed by the type -2 fuzzy neural network with GA and FCM-SVM. Thus, the type -2 fuzzy neural network with GA and FCM-SVM outperformed the existing approaches. The techniques implemented by

different authors may have some impediments that need to be considered such as low detection rate for least frequent attacks, computation time, speed, to handle the extended dimensions of data, etc. as shown in Table 2.

3.3. Hybrid Approach (Known and Unknown Attack Detection Phase):

The hybrid approach is the combination of known/signature-based detection and unknown/ anomaly-based detection in the network. This approach helps in detecting internal as well as external attacks. The working principle of the hybrid model comprises, the data packets are initially identified by the known attack detection phase i.e., snort and after the analysis, if the packet match with the existing database, then the packet is dropped. Contrarily, the packet is forwarded to the Unknown attack detection phase. Thus, the use of the hybrid approach is still uncommon in the field of cloud computing.

(Chiba et al., 2016) proposed a cooperative and hybrid NIDS designed for detecting malicious attacks in the cloud environment. The framework for NIDS includes Snort for signature-based and Back-Propagation Neural Network for anomaly-based intrusion detection. Snort helps in detecting known attacks and after detection of known attacks, Back-Propagation Neural Network (BPN classifier) is used for detecting unknown attacks. This approach helps in detecting DoS and DDoS attacks by sharing alerts in the central database. Thus, the detection time is reduced. The hybrid approach helps in reducing the computational cost by applying signature-based detection before anomaly-based detection. Packets from the physical and virtual networks are captured for detecting the intrusion. Initially, Snort was used for detecting the captured packets with the existing rules store in the signature database. If found any malicious activity, an alert is generated and stored in the central database, and the packet is discarded. The packets of non-intrusions are forward to the BPN classifier for detecting unknown attacks. The proposed system resulted in a high detection rate, accuracy, low false-negative, low false-positive, and reasonable computational cost.

(Olanrewaju et al., 2018) projected a rapid intrusion detection system that helps in detecting network attacks in less time. The proposed approach resulted in better performance. The techniques used for intrusion detection constitute the implementation of snort and the backpropagation neural network implemented using MATLAB. Initially, Snort worked for detecting renowned attacks. Later another technique of backpropagation is employed for detecting solely unknown attacks. Thus, the approach resulted in lesser time for detecting known and unknown attacks.

(Hatef et al., 2018) stated a hybrid network intrusion detection system that combines signature-based and anomaly-based techniques. This approach helps in the detection of internal as well as external attacks in the cloud environment. Initially, Snort is used to detect known attacks for the signature-based intrusion detection phase. The anomaly-based detection phase includes the c4.5 algorithm and quantization algorithm to detect unknown attacks. The working of the proposed approach is to first receive a packet in the network, in the first phase, i.e., the Snort will match the received data in the database. If the packet exists in the database, Snort will drop the packet with the notification to the admin. If the packet does not exist, it will be rerouted to the next phase, i.e., anomaly detection phase with the warning. The attack pattern will be stored in the known attacks database. If a similar

attack occurs in the system, snort would immediately detect it and take preventive action. Moreover, the Apriori algorithm is used to generate the pattern for the derived attacks. The proposed approach resulted in improved accuracy and reduced false alarm rate.

(Thierry et al., 2020) proposed a hybrid Intrusion Detection and Prevention System that detects and prevents signature-based attacks using the snort tool and anomaly-based attacks using a genetic algorithm. Snort combined with Splunk web-based framework for detecting and preventing DOS/DDOS attacks. This tool detects the attacks whose signature is already available in the database. And the second approach is used for anomaly-based intrusion detection and prevention using a genetic algorithm. This approach shows an improved IDS/IPS for the cloud environment that overcomes the security issues of cloud resources and service providers. Snort IDS results in lower performance than the genetic algorithm. The detection rate of Snort-IDS is between 49%- 99.97%, with a low false-positive, and the detection rate of the Genetic algorithm is over 90%.

Table 3 - Summary of intrusion detection and prevention system for Hybrid approach.

Reference	Approach	IDS Type	Detection Rate	Accuracy	Dataset	Advantage	Drawbacks
(Chiba et al., 2016)	Snort and Optimized Back Propagation neural network	CH-NIDS	N/A	N/A	CIDD	This approach reduces the computational time and cost.	This approach has not been implemented in real-time scenarios.
(Olanrewaju et al., 2018)	Snort and ANN with BPN	NIDS	N/A	DoS:97.3% Probe:95.1% U2R:99.8% R2L:93.3%	KDDCup'99	The computational time is reduced by using Snort.	Not implemented on huge dataset.
(Hatef et al., 2018)	Snort, clustering, c4.5 algorithm and Apriori algorithm	HIDS, NIDS	N/A	99.3%	NSL-KDD	This approach resulted in improved accuracy and reduced false alarms.	Increased computational cost.
(Thierry et al., 2020)	Snort with Splunk web framework and Genetic Algorithm	NIDS	99%	N/A	Real time traffic	This approach detects DoS/DDoS attacks with low FPR and FNR.	The proposed approach detects and prevents only DoS/DDoS attack.

N/A -Not Available

Various approaches are implemented with snort such as ANN, BPN, Apriori algorithm, etc. for known and unknown attack detection. The approach used with snort and ANN with BPN achieved better results compared with other techniques. Along with the benefits, some techniques have flaws such as not being implemented in a real-time scenario, not working on a large dataset, increased computational cost, etc.

4. Datasets For IDPS: There exist several important datasets for intrusion detection and prevention system.

1. **KDDCup'99:** This dataset is the modified version of the DARPA dataset. The dataset contains network traffic of seven weeks with 4 GB of tcpdump data that retains 5M records. The training dataset includes the standard data that has a wide variety of information labeled as an attack and normal that is simulated in the military

network environment. The dataset comprises of following types of attacks such as Dos, Probing, R2L, U2R (Lee et al., 2021).

2. NSL-KDD: The NSL-KDD dataset resolves the problem of the previous dataset by having few records in both the training and testing sets. KDDCup'99 dataset contains repetitious records in the training set that were removed in the NSL-KDD dataset. It prevents any bias in the classification and leads to an improved detection rate. This dataset may not work perfectly in real-time network traffic(Lee et al., 2021).

3. **ISCXIDS2012:** The dataset comprises profiles that retain the complete description of intrusions and the distribution models for protocols, lower-level network entities, and applications. The user behavior is analyzed by creating the profiles. These profiles can be used in inducing a dataset that includes the real-time traffic of SMTP, IMAP, HTTP, SSH, FTP, etc. This dataset contains both the malicious and normal activities of a network(Lee et al., 2021).

4. CSE–CIC–IDS2018: The dataset constitutes the attack scenarios for security attacks such as Web attacks, DDoS, Brute-force, etc. It also considers profiles for generating network traffic by the various protocols. There exist two types of profiles, M profiles and B profiles. M profiles represent the scenario for attacks. B profiles include the packet size, payload patterns, size, protocol's request time distribution such as HTTP, HTTPS, SMTP, IMAP, and SSH.

5. CICIDS2017: The dataset includes several records that resemble the real traffic data. It uses only B profiles for creating the profile of human behaviors. This dataset is built by protocols such as HTTP, SSH, HTTPS, email, FTP, etc. It can also hold the records of Web Attacks, Brute force, DDoS, etc.

6. **UNSW-NB15:** The dataset can be used to evaluate a Network intrusion detection system. IXIA software tool incorporated that can trace the normal and abnormal network traffic. This tool simulates nine types of security attacks and it also uses data of new attacks to be updated from the sites.

These are the datasets used for the intrusion detection and prevention system and each dataset provides the distinct restrictions and challenges for the better validations of results. Most of the related work of IDPS are based on KDDCup’99 and NSL KDD datasets and less work is done on the real-time traffic.

5. Research gaps in Existing Techniques:

1. The existing algorithms of intrusion detection systems resulted in a low detection rate for the least frequent attacks.
2. There exists a lesser number of approaches that examine computational speed.
3. The cloud environment has limited scope for the prevention of attacks.
4. For evaluating the existing approaches, a few parameters are considered such as accuracy, detection rate, etc.
5. Upgrading the performance parameters by consolidating the known attack detection phase and unknown attack detection phase.
6. Most of the implemented approaches used benchmark datasets that contain duplicate records and are not updated regularly.

7. Most of the implemented approaches used benchmark datasets that contain duplicate records and are not updated regularly.

8. Conclusion and Future Perspectives

This paper embraces different intrusion detection and prevention systems for the cloud computing environment based on existing tools and on computational intelligence techniques. For the identification of known/Signature-based attacks, Snort open-source IDPS can be used that resulted in less computational time and increased speed, and for the identification of Unknown/Anomaly based attacks, a combination of various approaches are used such as ANN and FCM, FCM and SVM, etc. Another technique for the identification of known as well as unknown attacks are the combination of both approaches such as snort with ANN or BPNN, GA, etc. The variety of studies that are mated out, signifies that the hybrid approach is better in performance. Several algorithms have succeeded in obtaining low false alarms, high accuracy, and in contrast, many algorithms once paired with others resulted in poor accuracy. Some of the existing techniques are not implemented in a real-time environment, are inadequate to prevent attacks, or have low computational cost and speed. Most of the organizations are using the existing tools for detecting only known attacks and minimal implementation is done for the unknown or novel attacks detection and prevention. In addition, the datasets used for intrusion detection are still lacking, and most of the work is based on KDDCup'99 and their variant. Thus, to secure the environment from malicious attacks there is a need of hybrid approach that can detect both Known/Signature based and Unknown/ Anomaly based attacks in the cloud environment for the real-time traffic. In future, we will conduct an extensive analysis of various computational intelligence techniques to provide better solution for the IDPS by taking real-time dataset.

Nomenclatures

IDS	Intrusion Detection System	CIDD	Cloud Intrusion detection dataset
IPS	Intrusion Prevention System	KDD	Knowledge discovery in database
ANN	Artificial Neural Network	DoS	Denial of Service
GA	Genetic Algorithm	U2R	User to root
FCM	Fuzzy C-means Clustering	R2L	Remote to Local
FNR	False Negative Rate	DDoS	Distributed Denial of Service
FPR	False Positive Rate	IaaS	Infrastructure as a Service
SVM	Support Vector Machine	SaaS	Software as a Service
BPNN	Back Propagation Neural Network	NIDS	Network Intrusion Detection System
HIDS	Host Intrusion Detection System		
IDPS	Intrusion Detection and Prevention System		

References

Alam, S., Shuaib, M., & Samad, A. (n.d.). *A Collaborative Study of Intrusion Detection and Prevention Techniques in Cloud Computing*. Springer Singapore. https://doi.org/10.1007/978-981-13-2324-9

Alhomoud, A., Munir, R., Disso, J. P., Awan, I., & Al-Dhelaan, A. (2011). Performance evaluation study of Intrusion Detection Systems. *Procedia Computer Science*, *5*, 173–180. https://doi.org/10.1016/j.procs.2011.07.024

Alturfi, S. M., Muhsen, D. K., Mohammed, M. A., Aziz, I. T., & Aljshamee, M. (2021). A Combination Techniques of Intrusion Prevention and Detection for Cloud Computing. *Journal of Physics: Conference Series*, *1804*(1). https://doi.org/10.1088/1742-6596/1804/1/012121

Bada, G. K., Nabare, W. K., & Quansah, D. K. K. (2020). Comparative Analysis of the Performance of Network Intrusion Detection Systems: Snort, Suricata and Bro Intrusion Detection Systems in Perspective. *International Journal of Computer Applications*, *176*(40), 39–44. https://doi.org/10.5120/ijca2020920513

Balamurugan, V., & Saravanan, R. (2019). Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation. *Cluster Computing*, *22*, 13027–13039. https://doi.org/10.1007/s10586-017-1187-7

Beigh, B. M., & Peer, M. A. (2014). Performance evaluation of different intrusion detection system: An empirical approach. *2014 International Conference on Computer Communication and Informatics: Ushering in Technologies of Tomorrow, Today, ICCCI 2014*. https://doi.org/10.1109/ICCCI.2014.6921740

Chiba, Z., Abghour, N., Moussaid, K., El Omri, A., & Rida, M. (2016). A Cooperative and Hybrid Network Intrusion Detection Framework in Cloud Computing Based on Snort and Optimized Back Propagation Neural Network. *Procedia Computer Science*, *83*, 1200–1206. https://doi.org/10.1016/j.procs.2016.04.249

Gaddam, R. T., & Nandhini, M. (2017). An analysis of various snort based techniques to detect and prevent intrusions in networks: Proposal with code refactoring snort tool in Kali Linux environment. *Proceedings of the International Conference on Inventive Communication and Computational Technologies, ICICCT 2017*, *Icicct*, 10–15. https://doi.org/10.1109/ICICCT.2017.7975177

Ghosh, P., Shakti, S., & Phadikar, S. (2016). A Cloud Intrusion Detection System Using Novel PRFCM Clustering and KNN Based[1] P. Ghosh, S. Shakti, and S. Phadikar, "A Cloud Intrusion Detection System Using Novel PRFCM Clustering and KNN Based Dempster-Shafer Rule," Int. J. Cloud Appl. Comput., vol. . *International Journal of Cloud Applications and Computing*, *6*(4), 18–35. https://doi.org/10.4018/ijcac.2016100102

Hatef, M. A., Shaker, V., Jabbarpour, M. R., Jung, J., & Zarrabi, H. (2018). HIDCC: A hybrid intrusion detection approach in cloud computing. *Concurrency and Computation: Practice and Experience*, *30*(3). https://doi.org/10.1002/cpe.4171

Jaber, A. N., & Rehman, S. U. (2020). FCM–SVM based intrusion detection system for cloud computing

environment. *Cluster Computing*. https://doi.org/10.1007/s10586-020-03082-6

Khamphakdee, N., Benjamas, N., & Saiyod, S. (2014). Improving intrusion detection system based on Snort rules for network probe attack detection. *2014 2nd International Conference on Information and Communication Technology, ICoICT 2014*, 69–74. https://doi.org/10.1109/ICoICT.2014.6914042

Lee, S. W., Mohammed sidqi, H., Mohammadi, M., Rashidi, S., Rahmani, A. M., Masdari, M., & Hosseinzadeh, M. (2021). Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review. *Journal of Network and Computer Applications*, *187*(December 2020), 103111. https://doi.org/10.1016/j.jnca.2021.103111

Mell, P., & Grance, T. (2011). The NIST-National Institute of Standars and Technology- Definition of Cloud Computing. *NIST Special Publication 800-145*, 7.

Mishra, V., Vijay, V. K., & Tazi, S. (2016). Intrusion detection system with snort in cloud computing: Advanced IDS. *Advances in Intelligent Systems and Computing*, *408*, 457–465. https://doi.org/10.1007/978-981-10-0129-1_48

Modi, C. N., Patel, D. R., Patel, A., & Rajarajan, M. (2012). Integrating Signature Apriori based Network Intrusion Detection System (NIDS) in Cloud Computing. *Procedia Technology*, *6*, 905–912. https://doi.org/10.1016/j.protcy.2012.10.110

Olanrewaju, R. F., Islam Khan, B. U., Najeeb, A. R., Ku Zahir, K. N. A., & Hussain, S. (2018). Snort-based Smart and Swift Intrusion Detection System. *Indian Journal of Science and Technology*, *11*(4), 1–9. https://doi.org/10.17485/ijst/2018/v11i4/120917

Pandeeswari, N., & Kumar, G. (2016). Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN. *Mobile Networks and Applications*, *21*(3), 494–505. https://doi.org/10.1007/s11036-015-0644-x

Raja, S., & Ramaiah, S. (2017). An Efficient Fuzzy-Based Hybrid System to Cloud Intrusion Detection. *International Journal of Fuzzy Systems*, *19*(1), 62–77. https://doi.org/10.1007/s40815-016-0147-3

Samriya, J. K., & Kumar, N. (2020). A novel intrusion detection system using hybrid clustering-optimization approach in cloud computing. *Materials Today: Proceedings*, *xxxx*. https://doi.org/10.1016/j.matpr.2020.09.614

Sengaphay, K., Saiyod, S., & Benjamas, N. (2016). Creating snort-IDS rules for detection behavior using multi-sensors in private cloud. *Lecture Notes in Electrical Engineering*, *376*, 589–601. https://doi.org/10.1007/978-981-10-0557-2_58

Shah, S. A. R., & Issac, B. (2018). Performance comparison of intrusion detection systems and application of machine learning to Snort system. *Future Generation Computer Systems*, *80*, 157–170. https://doi.org/10.1016/j.future.2017.10.016

Shamshirband, S., Fathi, M., Chronopoulos, A. T., Montieri, A., Palumbo, F., & Pescapè, A. (2020). Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review,

taxonomy, and open research issues. *Journal of Information Security and Applications*, *55*(September). https://doi.org/10.1016/j.jisa.2020.102582

Singh, P., & Ranga, V. (2021). Attack and intrusion detection in cloud computing using an ensemble learning approach. *International Journal of Information Technology (Singapore)*. https://doi.org/10.1007/s41870-020-00583-w

Snehi, J., Bhandari, A., Baggan, V., & Snehi, M. (2020). Diverse Methods for Signature based Intrusion Detection Schemes Adopted. *International Journal of Recent Technology and Engineering*, *9*(2), 44–49. https://doi.org/10.35940/ijrte.a2791.079220

Srilatha, D., & Shyam, G. K. (2021). Cloud-based intrusion detection using kernel fuzzy clustering and optimal type-2 fuzzy neural network. *Cluster Computing*, *9*. https://doi.org/10.1007/s10586-021-03281-9

Thilagam, T., & Aruna, R. (2021). Intrusion detection for network based cloud computing by custom RC-NN and optimization. *ICT Express*, *xxxx*. https://doi.org/10.1016/j.icte.2021.04.006