A Comparative Analysis of Different Intrusion Detection Techniques in Cloud Computing

Aditya Bakshi[1](✉) and Sunanda[2]

[1] Lovely Professional University, Phagwara, India
addybakshi@gmail.com
[2] Shri Mata Vaishno Devi University, Katra, India

Abstract. Nowadays, the foremost optimal choice of every IT organization is cloud computing. Cloud computing technology is very flexible and scalable in nature. The prime concern in cloud computing is its security and privacy, because intruders are trying to breach it. The main reason for breaching is its open and distributed architecture. For detection of various attacks on cloud, the most common mechanism used is Intrusion Detection System (IDS). We have presented a comparative analysis of some existing cloud based intrusion detection systems and different methods of deploying the IDS are used for overcoming the security challenges. In spite of the fact that there are various existing literatures in this area of study, we endeavor to give more intricate picture of a thorough analysis. This paper shares an overview of different intrusions in cloud. The metrics, which are used for comparative analysis, are of various types like positioning, detection time, detection techniques, data source and attacks. The comparative analysis also shows the limitations of each technique that tells whether the cloud-computing environment is secure or not.

Keywords: Cloud computing · Firewall · Detection techniques
Data sources · Intrusion detection system

1 Introduction

Cloud computing is the latest computing technology which provides various services on demand and pay per use basis. Fundamental idea behind the evolution of this technology is diversity of computing relative to users. Every user has his own needs and expectations about the services. To fulfil their need, various features from computing components i.e. software, hardware and network are required. It is almost impossible to have distinguish computing environment for every user. Each client or user requirements are diverse i.e. on demand services or highly paid services from network; software development organizations cannot purchase every development environment for clients. As the technological advancements are increasing at a very fast rate, this lead to the evolution of cloud computing environment where all the services can be provided to the client in virtual environment. There are cloud servers created and maintained by computing giant firms, which provide numerous services required by users. Basically, cloud services are categorized in three broad categories. First one is Software as a Service (SaaS) which provides various applications especially bounded

A. K. Luhach et al. (Eds.): ICAICR 2018, CCIS 956, pp. 358–378, 2019.
https://doi.org/10.1007/978-981-13-3143-5_30

to software to users. Second one is Infrastructure as a Service (IaaS) which provides various infrastructure environments to users and last one is Platform as a Service (PaaS) which deals with various platforms like OSs, etc. [4, 5]. All these services are available to users on pay per use and on demand basis, which helps the users to get the services at minimum cost that is impossible to get at affordable price in the past. Users have to just pay the rent for the time to which they are using services. Apart from this unique feature, cloud computing provides various other features like availability, maintainability, scalability, interoperability, etc. Not these all facilities can be achieved anyhow by standalone users in their local infrastructure due to various unavoidable conditions whereas cloud providers support them due to devoted services.

2 Common Attacks in Cloud

Cloud computing is the next generation technology, which is suitable for varied users having different resource and operating requirements [1]. The platforms for the cloud, computing are attractive because they are different from the traditional physical infrastructure on the basis of on-demand resources such as purchase, installation, configuration and deployment etc. Moreover, due to the openness behavior (i.e. data privacy for individuals) of the cloud, there are various security issues architecture that involves network as Internet and intranets Some of the major intrusions are described as follows:

Insider Attack: This attack is performed by insider cloud users i.e. It enters to the system by legitimate authorization. As, this attack is performed by some insider, the prediction and lethality of an attack is very difficult to find. Users may try to breach the security of cloud by gaining unprivileged access by using their credentials. Such attack covers the data tempering, deletion of critical assets and spreading of falsified information to hamper the system etc. This is one of the most disastrous threat to cloud because once the internal security architecture will be breached then overall system can be compromised easily.

Flooding Attack: For providing stability to the internet service, the flooding attack is considered to be the major challenge in cloud computing environment. In this attack, attacker frequently flood the huge amount of data packets to choke the network system. The data may include the ICMP, TCP, UDP packets etc. which are sent to just flood the system and gain access to other resources [2]. The two major techniques used for the flooding attack are DoS (Denial of service) and DDoS (Distributed denial of service) attack. Flooding of packets on server by one computer is called as denial of service attack whereas the same process to be done from many computers is called distributed denial of service attack.

User to Root Access: In this attack, those users are compromised which are having root access to the cloud system. In this attack, attacker can perform administrator level work for accessing the root level permissions and compromising the user credentials [3]. However it is not a single attack based on paradigm that will be applied on the cloud system. User to root access attack also involves many techniques like eavesdropping etc. The main motto behind this attack is to gain credentials to reach to the root level of the cloud server which can be further compromised by using the same.

Port Scanning: Port scanning is the technique to scan all ports of any system. Although it is a manual process to check for each and every port and their status as open or close. There are various automated tools such as nmap, wireshark and tcpdump which provide detailed description about the port numbers that can be incorporated with IP address [3]. These tools are sometimes used to attack on the cloud environment. If not all open ports are being used by any specific service, that ports can be used as a back door. In backdoor, the attacker inserted the malicious code for gaining access the network system.

Attacks on Virtual Machine (VM) or Hypervisor: Cloud environment is completely based on virtual architecture. It virtualizes both the environments either internal or external. Virtual machine is a dedicated machine that works virtually on behalf of real environment. The most popular technique for clubbing and splitting VMs is based on hypervisor. A hypervisor is a virtual machine manager that allows multiple operating system runs on a single host system at a same time. There are various known attacks which try to compromise either VMs or target hypervisor to completely choke the system. The attacker always target the middle layer that works between the upper and lower layer in VMs. If the attackers can compromise any one of these three layers then he would result compromise the whole system very easily.

Apart from the above discussed attacks there are various other attacks which lead to severe security problems. The common solution to the problem is firewall implementation. However it does not solve the problems at all which forces the intrusion detection system (IDS) or sometimes intrusion detection and prevention system (IDPS) implementation. First of all we see the features of firewall and various other firewalls which can be implemented and then after various other IDPSs and their comparison in cloud environment [7].

3 Firewall

Firewall comprises various set of rules which act as the first line defence mechanism involved in the system. It protects and filters all the incoming and outgoing requests from the system. However, it is completely static in nature working on the pre-defined rules of network. It is unable to protect the system in cases where requests are evasion in nature and here IDPSs play crucial role for the system [8, 9]. Some of the major firewall techniques that are used in cloud environment are Static Packet Filtering Firewall, Stateful Packet Filtering Firewall, Stateful Inspection Firewall and Proxy Firewalls [10].

Firewalls restrict to some extent in security attacks but not as an overall solution. For sustaining more security in different types of attacks, IDS or IPS can be served as solution that could be incorporate in cloud. However, the different parameters and techniques are required for improving the efficacy of an IDS/IPS in cloud computing. The parameters comprises of different techniques used in IDS and its configuration within the network. Some traditional IDS/IPS techniques such signature based detection, anomaly detection, state protocol analysis etc. can also be incorporated in cloud. The next section covers the common IDS/IPS techniques.

4 Cloud Based IDS Techniques

4.1 Signature Based Detection

This technique incorporates signatures of various known attacks. These signatures are stored in database server of IDS and any incoming or outgoing requests are matched with them. Any matching signature request is discarded immediately from the network or other consequences may be applied like changing the contents, modifying the target, etc. However, it is the best technique for known attacks but proves to be very ineffective in case of unknown attacks. Any attack or security breach, which is attempted by modifying the content, is unable to be detected by this technique. One of the key reason for using signature-based detection is because its rules can be easily reconfigured. Reconfiguration of rules is required for updating the signatures of unknown attacks. These signatures are helpful for detecting the network traffic [11].

In cloud, the known attack can be easily detected by using signature based intrusion detection technique. The signature-based technique is applied on the front end of cloud for detecting the external intrusion or at back end of cloud for detecting internal intrusions. If signatures are not updated, it cannot be used to detect unknown attacks in cloud. Different signature based detection approaches along with the methodology adopted and salient features are shown in Table 1. All approaches in tables tells about the methodologies that have been used to provide the security in cloud environment. Jia et al. [14] proposed an efficient revocable ID-Based Signature scheme that is performed on cloud revocation server. In this approach, large prime numbers are used to provide the greater security. The main advantage of this approach is that it uses less time consumption for detection of unknown attacks than other traditional techniques. Arjunan et al. [15] proposed an enhanced intrusion detection approach for securing of networks by incorporating correlation module (CM) and management module (MM). This technique is used for both anomaly based and signature based detection attacks. Hamdi et al. proposed cloud based signature learning service approach using inductive logic programming.

The results for this technique is better than previous technique as it automatically generates the signature for SNORT IDS [16]. Table 1 shows different Signature based detection approaches along with their methodologies and salient features.

4.2 Anomaly Detection

Anomaly detection technique tries to detect intrusions that are anomalous to the actual definition. This technique involves various profiles that are used to filter the traffic as genuine or malicious activity.

All such profiles are stored in advance as well as dynamically updated based on the uses and traffic pattern. Some of the known products based on this technique are working very well in real life scenarios [12].

Apart from the normal computing, it is also very useful in case of cloud computing. It involves data collection related to the behavior of legitimate users over training period, and then applies various test, which are statistical in nature, are used to observe behavior and determines genuine user. It is very useful in cases of unknown attacks

Table 1. Signature based detection approaches and their comparison

Reference	Methodology adopted	Salient features
[14] Efficient revocable ID-based signature with cloud revocation server	The proposed model uses RIBS scheme which is composed of 4 phases namely I. Setup: used for generating master key and master time key II. InitKeyExt: for sending the initial key to the user through a secured channel III. TimeKeyUpd: the cloud based server will computes the time update key and send it back to the user IV. Sign: the signer will finally sign the message with the given user key and time update key	- A revocable IBS scheme is proposed in which the revocation functionality is done on a Cloud Revocation Server (CRS) - To ensure appropriate security level, large prime numbers (512 & 160 bits) have been used - The proposed model is less time consuming compared to the traditional techniques - Hash functions used are much more efficient and have shorter signature size than the previous models - Suitable for resource constrained devices such as wireless sensors
[15] An enhanced intrusion detection framework for securing network layer of cloud computing	The proposed system consists of different security modules like *management module, correlation module* and NIDS Correlation Module (CM) is used to detect distributed attacks at each cluster node Management Module (MM) is used to gather the distributed attack evidences from cluster nodes The NIDS is used to monitor the physical as well as virtual network traffic A network traffic profile will be generated from the capture packets	- Combines signature based and anomaly based detection techniques - Snort is used for Signature based detection, and different classifiers such as decision tree, naïve bayes, random forest, linear discriminant analysis and random forest are used for anomaly based detection - Uses Dempster Shafer Theory (DST) for making final decision on collected intrusion evidences from the cloud
[16] A cloud-based architecture for network attack signature learning	- The Learning Nodes (LN) provides the signature learning service - It will record the network traffic in a PCAP format which will be translated using prolog rules	- Cloud based signature learning service using inductive logic programming is proposed - Predicates were formed in order to describe signature of different attack vectors in the system

(*continued*)

Table 1. (*continued*)

Reference	Methodology adopted	Salient features
	- The Inductive Logic Programming (ILP) engine is present inside the learning node along with the Background Knowledge (BK) database and a Grammar Translator Proxy - The existing prolog signature rules are transformed into SNORT signature rules - Finally the signature is sent to the user and gets feed into its signature database	- Results have shown that the proposed framework has successfully been able to automatically generate signatures of SNORT IDS
[17] Event pattern discovery on IDS traces of cloud services	- Authors have applied Growing Hierarchical Self Organizing Maps (GHSOM) technique - Initially, the network data traffic is collected using IDS/Honeypot traces - Data is clustered using GHSOM and a series of visualization; feature observation and even pattern discovery are performed	- Unsupervised learning techniques are used for classifying network data more efficiently - GHSOM technique helps in efficient data analysis - Effectively discovers different critical attack vectors and efficiently reduces the trace log size

where definitions or any specific signatures are unknown in advance. The main idea behind use of this detection technique is to decrease the false alarm rate and work either perfectly either with known or unknown attacks [13]. Anomaly detection techniques detects unknown and known attacks, which are segregated at different levels. In cloud, by using anomaly based detection, large number of events that can (network level or system level) occur, which makes difficult to monitor or control intrusion [1].

Capability of soft computing to deal with uncertain and data that is partially true, makes them very useful technique in intrusion detection. There are various techniques from this computing like Fuzzy Logic, Association rule mining, Artificial Neural Network (ANN), Genetic Algorithm (GA), Support Vector Machine (SVM), etc. that can be incorporated to improve the accuracy of detection and efficiency of anomaly detection based IDS and signature based IDS. Sunita et al. [19] uses k-learning classification over cloud to improve detection accuracy of anomaly based IDS. It uses Bayesian classifier, which converges quicker than other discriminative models and requires less model training time.

Suaad et al. [20] proposed a unique model of detecting anomalies in IaaS environments by monitoring the VM in cloud system. Their detection system proved very

Table 2. Anomaly based detection approaches and their comparison

Reference	Methodology adopted	Salient features
[18] Intrusion detection and prevention system using K-learning classification in cloud	- The proposed model uses cloud based hybrid architecture to improve the intrusion detection accuracy - Data packets are logged and checked against the rules over the cloud platform - Log files are divided into two datasets for testing and training purpose - K2 learning algorithm is applied on the obtained datasets and Bayesian algorithm is used for creating a junction tree - Finally check the new connections are checked against the given threshold value are datasets will be updated accordingly	- Snort is used as an intrusion detection tool - Filtering rules are logged onto the cloud server - log files are used as training data set in weka - K2 learning algorithm is used for training the data - Junction tree is created using Bayesian algorithm - Results thus obtained are categorized into two types, namely: users and services - Graphs are plotted for showing anomalous users as well as services used
[19] Detecting anomalies in IaaS environments through virtual machine host system call analysis	The IaaS environment is monitored using the following setup - A single cluster setup is used which consists of 3 servers as well as a network infrastructure of switches and routers - Server 1 contains all the cloud components and acts as the gateway of cloud network; server 2 hosts the entire client VMs and acts as a node controller - Server 3 is used for management and initiation VMs - All the system calls issued by clients are recorded using Linux strace mechanism - Normal behavior profile for each VM is maintained using collected data and classifier is trained	- System calls are monitored at the VM level without any arrangement within VMs - Level of granularity is higher and sufficient to detect a relevant number of attack vectors - Linux KVM-based references are used for conducting experiments and statistical analysis - Unlike the previous research studies, the proposed system does not require any knowledge about the VM or the underlying OS - System is successfully able to categorize normal and anomalous system calls

(*continued*)

Table 2. (*continued*)

Reference	Methodology adopted	Salient features
	- Finally, the system is tested by generating some anomalous system calls	
[20] Preventing mistraining of anomaly-based IDSs through ensemble systems	- Proposed an ensemble classifier for preventing the mistraining of a classifier - One classifier is trained online with the incoming data and other is trained offline with its initial decision rules - Experiment is performed on distributed IDS EMERALD that uses Bayesian inference for its decision making process - System is tested by generating multiple mistraining attacks and measured according to the amount if false positives and negatives	- Anomaly based IDS is trained online according to the nature of incoming data traffic - Ensemble classifier is proposed which contains multiple copies of a single classifier - EMERALD IDS is used for conduction the experiment - Mistraining attacks includes target integrity attacks and red herring attacks
[22] Machine learning for anomaly detection and categorization in multi-cloud environments	Their work comprises of four different stages: - Detection of anomalous packets from normal traffic - Test whether the detected attack is generic to avoid any misclassification of attack vectors - Attacks are categorized as Shellcode, Reconnaissance and Backdoor attacks - Classification algorithm further distinguishes Reconnaissance attacks from rest of the network traffic	- Detection as well as categorization of anomalies is done - Machine learning techniques utilized by their learning model are Random Forest (RF) and Linear Regression (LR) - Achieved detection accuracy of 99% and accuracy for categorization of anomalies is 93.6% respectively - The proposed technique can be applied in multi-cloud environments - Dataset used was of UNSW, which is publicly available for comprehensive study

successful in classifying normal and anomalous behavior than other cloud-based approaches. Pan et al. [22] gives a beautiful categorization of several different attacks which was absent in many of the past researches. In addition, they further segregates the attacks and prevents any misclassification of attack vectors. Different anomaly based detection approaches are shown in Table 2. The table shows the comparison and methodologies of all the anomaly based detection approaches along with salient features.

4.3 Artificial Neural Networks (ANN) Based IDS

ANNs generalizes data from incomplete data for intrusion detection classifier as normal or intrusive behavior. Types of ANN are used in IDS are: Back Propagation (BP), Multi-Layer Feed-Forward (MLFF) nets and Multi-Layer Perceptron (MLP). Distributed Time Delay Neural Network (DTDNN) has been claimed as the best detection technique in this category until now. It contains capability of classifying and fast conversion rates of data and proves to be a very simple and efficient solution. Its

Table 3. ANN based detection approaches and their comparison

Reference	Methodology adopted	Salient features
[23] An efficient approach of trigger mechanism through IDS in cloud computing	- Information Theoretic Model (ITM) is used to detect any intrusion over cloud network - Data stream is marked as intrusive or normal using state transition diagrams - Misuse detection is used to detect anomalies by comparing with existing obtrusion signature - In case any intrusion is detected, alarm is raised - The action engine is responsible for taking valid action	- Efficient triggering mechanism that uses Artificial Neural Networks (ANN) and Information Theoretic Model (ITM) - Uses State transition diagrams and Misuse detection engine to identify any unapproved event over cloud network - Gives better execution results over other triggering mechanisms in cloud computing environment
[24] A neural network based distributed intrusion detection system on cloud platform	- Firstly, the neural network is trained using KDD dataset - The IDS then receives instruction signals for making intrusion detection tasks for the given 5-node architecture - After the training phase, ANN performance is tested using KDD no-label dataset and corrected dataset - The output thus obtained will help in determining whether there is any malicious actions as well as what kind of attack vector is captured	- ANN based distributed IDS to make full utilization of available resources - Capable of detecting new kinds of attack vectors with genuinely precise results within acceptable time limits - Accuracy for classifying whether activities are normal or malicious in nature is 100% - Promising way for identifying new attack vectors in cloud platforms

accuracy can be improved by combining various other techniques related to soft computing.

ANN based solutions of IDS proves a better solution over other techniques for network data which are unstructured in nature. Accuracy of intrusion detection involved with these techniques is completely dependent on training profile and layers that are hidden. Gupta et al. [23] proposed an efficient triggering mechanism that uses ANN and ITM model to detect any intrusion over the cloud. It gives better results over other triggering mechanisms in cloud environment. However, their system lacks the capability of attack categorization. ANN based detection approaches and their comparison is shown in Table 3. Li et al. [24] proposed a distributed IDS for cloud platforms that performed better than ITM model when comes to detection of new kinds of attack vectors.

4.4 Fuzzy Logic Based IDS

FIDS are used for detecting and inspecting various network traffic related to SYN and UDP floods, Ping of Death, E-mail Bomb, FTP/Telnet password guessing and port scanning. Some evolving techniques under Fuzzy Neural Network (FuNN) collaborates both type of learning as supervised and unsupervised learning [1]. EuFNN has better accuracy in intrusion detection than normal ANN techniques and experimental results shown in [1] prove accuracy. Real time intrusions can be also detected in real time environment by involving association rules of Fuzzy System. The experimental results generate two result sets that are mined online from training data. It is very suitable for DoS or DDoS attacks that are implemented on large scale. Alqahtani et al. [26] have examined popular IDS framework using different classifiers against each other to identify the most effective classifier in detecting various attacks. Their results shows that SuricataIDS when used with decision-based classifier gives the highest accuracy among other classification mechanisms. Mary et al. [27] have used fuzzy logic control for building multi-layer trust security model, which unlike previous fuzzy based systems is capable of faster classification with higher degree of accuracy. Fuzzy based detection approaches and comparison is shown in Table 4.

4.5 Association Rule Based IDS

There are various intrusions that are formed based on known or variants of known attacks. Apriori algorithm for determining the signatures of such attacks are used and they are also capable to determine the variants of such attacks can be determined and detected by frequent item sets. Data mining technique used in Network based intrusion detection with signature-based algorithm generates signatures for misuse detection.

However, drawback of the proposed algorithm is involved time consumption, which is more than considerable for generating signatures. Scanning reduction algorithm solved this problem, which reduces the number of database scans for effectively generating signatures from previously known attacks. However, there are very high false positive rates occur which generate due to unwanted and unknown patterns.

Table 4. Fuzzy based detection approaches and their comparison

Reference	Methodology adopted	Salient features
[25] A comparative analysis of different classification techniques for cloud intrusion detection systems' alerts and fuzzy classifiers	- The main aim of this research is to compare different IDS using certain number of classifier algorithms to check which one is better - They have tested different IDS like Snort, Suricata, FL-Snort and FL-Suricata using different classifiers such as Naïve Bayes, Decision Tree, K-NN and OneR - First step is to rank every class of attack and compare them based upon following metrics: 1. Accuracy 2. Precision 3. Sensitivity 4. Specificity 5. F-measure - The second step was to compare the given IDS one by one against each other and conclude that which IDS works better in identifying attack vectors with each classifier	- Popular IDS framework are examined extensively using different classifiers - Classifiers taken were: Naïve Bayes Decision Tree K-Nearest Neighbor OneR - IDS frameworks used are: Snort Suricata FL-Snort FL-Suricata - Experiments were carried upon ISCX dataset on WEKA platform - Decision Tree classifier gives the highest accuracy of 99.5% among all the four classification mechanisms
[26] A comparative study of different fuzzy classifiers for cloud intrusion detection systems' alerts	- Firstly, they have categorized the ISCX dataset into different categories like, Normal, Infiltrated, HTTP DOS, DDOS, and Brute Force - They run this dataset on Snort as well as Suricata IDS in offline mode - After obtaining the results, to get more accuracy in categorizing different attack vectors they have built IDS fuzzy classifiers - Finally the attack vectors were categorized more	- Their main goal was to identify unique sorts of network attacks inside MyCloud network using two most popular IDS frameworks namely, Snort and Suricata - A Fuzzy logic system is proposed to better classify different attack vectors - Different performance metrics were chosen like accuracy, sensitivity, specificity and false alarm rate

(*continued*)

Table 4. (*continued*)

Reference	Methodology adopted	Salient features
	accurately based on the analyzed alert files	- In depth comparison between different classifier based IDS is given
[27] Fuzzy logic approach to modelling trust in cloud computing	- Proposed a multi-layer trust security model (MLTSM) based on fuzzy logic control - Trust evaluation across three layers namely IaaS, PaaS and SaaS is done - Trust value is obtained through data center policy (DCP), Secure Shell (SSH) and intrusion detection/prevention ID. - Fuzzy logic control is used to evaluate the degree of membership whose value lies between 0 and 1, where 0 signifies low security and 1 signifies high security	- Their model MLTSM is capable of enhancing the protected deployment of cloud framework in mission critical applications such as military, threat management etc. - Its experimental results confirms coordinate assurance and verification of trust condition of any given distributed computing administration - Proved valuable for correlation, arrangement and enhancing end-client trust in choosing or devouring distributed cloud based computing resources

4.6 Support Vector Machine Based IDS

SVM is better than other artificial intelligence techniques used with IDS. There are various available experiments, which shows its efficiency over other techniques. It uses limited sample data to detect intrusions where accuracy does not get affected due to dimensions of data. False positives rate is also very less than other techniques as experimented in [6].

This is because that various other techniques require large sample dataset whereas it works on a limited sample dataset. It uses limited sample data to detect intrusions where accuracy does not get affected due to dimensions of data. False positives rate is also very less than other techniques as experimented in [6]. This is because that various other techniques require large sample dataset whereas it works on a limited sample dataset. SVM works on binary data so for better accuracy, it can be combined with other techniques which can improve its accuracy in detection. SVM is combined with SNORT and some basic rule sets of firewall, which allows it to generate a new and effective technique for intrusion detection.

The SVM- classifier is also used with SNORT to reduce false alarm rate and improve accuracy of IPS. SVM IDS techniques can prove the best techniques for intrusion detection in cloud, which can enhance its current feature and extends its security level up to a considerable level. Raneel et al. [28] proposed a similar study [19] for the protection of VMs over Infrastructure-as-a-Service (IaaS) environments but uses

SVM classifiers. They presented a thorough study of different classes of DoS attacks and were capable of detecting these attacks in cloud platforms. Mukkavilli et al. [29] proposed a theoretical model for detecting anomalous changes in network traffic by

Table 5. SVM based detection approaches and their comparison

References	Methodology adopted	Salient features
[28] Detecting denial of service attacks in the cloud	The proposed approach is implemented in the following manner: - First an IaaS (Infrastructure as-a Service) cloud is created - A testbed is selected for this cloud platform consisting of VMs. Of those VMs, some are normal and some are furnished with DoS attack tools - This framework will monitor all the outgoing and incoming network traffic and generates an alert to the cloud admin in case if denial of service attack is detected	- Novel approach for the protection of virtual machines (VMs) against DoS attacks - Eucalyptus is the open source cloud platform used for carrying out this experiment - A novel IDS is proposed which contains different features such as: feature extraction, packet sniffing and SVM classification - Different DoS attacks detected includes: - Ping of Death - ICMP flooding attack - TCP SYN flooding attack - TCP LAND - UDP flooding attack - DNS flooding attack
[29] Mining concept drifting network in cloud computing environments	- A test environment is made for processing data and converting it into LIBSVM (SVM library) format - Dataset used is KDDSUBSET, LBNL and DARPA - Manual dataset is also created using “tcpdump” -Cloud environment is set up for getting real time data using Amazon Web Services (AWS) - Captured data is classified as attacks based on certain behaviors	- Theoretical model for integrated supervised machine learning and control over cloud platform for detection of drift in network traffic pattern is presented - Different components in the proposed model includes: Kullback Leibler, divergence based relative entropy scheme, an online SVM classifier, anomaly based IDS and feedback control engine - Proposed model will report any alert only, if there is a significant changes in the traffic pattern, and does not report any minor changes

(*continued*)

Table 5. (*continued*)

References	Methodology adopted	Salient features
[30] Combined analysis of support vector machine and principle component analysis for IDS	- Firstly data is collected and normalized and passed through the PCA (Principle Component Analysis) - PCA further categorize the data into normal or attack vector using a predefined threshold value - The selected dataset (KDD99) is used for training and testing purpose - Finally the data is saved and used for detecting future attack vectors with similar attacking patterns	- A controlling mechanism is proposed for wireless data using IDS - Concept of Principle Component Analysis (PCA) is used for detecting attack vectors and intrusion detection in smart grid - Multiple factors considered are: rate of increase in network efficiency, response time, rate of increase in system error and differences in usage of PCA respectively - PCA technique gives better results than most of the conventional schemes and usage of SVM enhances the overall performance of IDS and decreases the overall analysis time

using supervised machine learning and SCM classifier over cloud environment. Their system is susceptible to higher false positive rates. Raja et al. [30] proposed a novel approach of using Principle Component Analysis (PCA) for detecting attack vectors over cloud platforms. Their approach gives better results than most of the conventional SVM based classifiers and decreases overall analysis time. Different SVM based detection approaches and their comparison is shown in Table 5.

4.7 Genetic Algorithm Based IDS

Genetic Algorithms (GA) use confidence based fitness functions for intrusion detection, which classifies network in a very efficient manner. These values can be used and determined for the profile generation as well. These services are very much useful in cases where intrusion behaviors are very dynamic in nature. These techniques can be collaborated with other techniques, which are resource intensive and prioritize the overall performance of the system. These techniques use training period and determine the fitness value based on the trained profiles. However, GA can be integrated with other such techniques for better results in cloud technology.

This feature is more important than any other techniques involved for intrusion detection. It is also suitable in scenarios wherever there is a need of mutual authentication in cloud among users. Most of the genetic algorithms uses techniques, which are derived from biological concepts like mutation, inheritance, crossover and selection. Fan, Yu et al. [31] proposed a cloud-based platform called T-DNA Tagged Rice

Table 6. Genetics based detection approaches and their comparison

References	Methodology adopted	Salient features
[31] TTRSIS: a cloud computing platform for rice functional genomics research through a reverse genetics approach	The Genomic analysis is carried out using the following procedure: i. BLASTN (Basic Local Alignment Search Tool) is used for the identification of T-DNA and binary vector procedures ii. Rice GAAS (Genome Automated Annotation System) is utilized to obtain Rice genomic sequences iii. Align module utilized BLASTN search to find sequences match to RB region iv. Search module is used for providing search options for gene id, gene name, and mutant line number v. Rice gene functional characterization module makes the functional characteristics of rice genome as current as possible vi. Physical distribution module provides rice seed distribution and inventory for academic research	- TTRSC is established in Asia University to with the administration, protection and circulation of mutant rice seeds stock - It is used for handling the genomic information produced from Taiwan Rice Insertional Mutagenesis (TRIM) - TTRSC consists of four modules: i. Align module ii. Rice quality module iii. Physical distribution module iv. Search module - TTRSC helps academicians and scientists to query intrigued genes stored 21 Kb downstream or upstream of T-DNA addition sites
[32] Genetic algorithm based feature selection algorithm for effective intrusion detection in cloud networks	- A new genetics based feature selection algorithm is proposed using Fuzzy SVM (Support Vector Machines) - The GA find and eliminates any redundant features which ultimately reduces the training time and ambiguousness - Next the feature selection search is used to add and/or remove unwanted features into the framework - Then a search strategy is decided like complete, random and sequential	- Novel IDS which uses genetics based feature detection and Fuzzy SVM based classification mechanism - Overall runtime is reduced by selecting only important features using the feature selection module - Reduction in runtime improves the accuracy of the classification mechanism done through SVM classifier - Final execution outcomes when tested with KDD Cup 99 dataset, using the

(*continued*)

Table 6. (*continued*)

References	Methodology adopted	Salient features
	- Finally a subset is generated, which is evaluated using certain evaluation criteria. These criteria could be information, distance, dependency etc. - A stopping condition is used when any of the given condition is met. Like when the maximum number of iterations are completed etc.	proposed classification and feature detection mechanism results in higher detection rate and a reduced false alarm rate
[33] A classification algorithm based on ensemble feature selections for imbalanced-class dataset	The following algorithm (IESF) has been adopted by the authors: - A subset of random feature is generated along with a classifier L - Ensemble prediction results are gained from the testing example - Initial objective function is calculated and classifier i is flipped over its jth index - New ensemble is gained from the testing example and value of the objective function is re-calculated - Search will be stopped when all the features are over or it reaches the number of configured loops	- Novel classification mechanism for solving imbalanced class dataset called Ensemble Feature Selection (EFS) - Proposed system uses the predominance of EFS in precision, at that point considers the decent variety and unevenness in the outlining proper component subset target capacity to make it fit for the imbalanced dataset - To compute accuracy of the system, it picks the class oriented F-measurement and ingresses a punishment-reward algorithm into KW diversity estimations

Service Information System (TTRSIS) for research based on rice genomics using Genome Annotation System (GAAS). Their system helps researchers and scientists to query genes stored 21 Kb downstream or upstream of T-DNA addition sites. Kannan et al. [32] proposed a novel mechanism that uses genetics based feature detection and SVM based classifier, which improves the classification accuracy when compared to other techniques by selecting only important features. The running time is reduced by removing unnecessary features with the help of feature selection module. The proposed system has a higher detection rate and reduced false alarm rate. Yin et al. [33] proposed a novel classification mechanism for solving imbalanced class dataset and shows a higher accuracy when compared to other conventional algorithms. Different Genetic based detection approaches along with their comparison is shown in Table 6.

Table 7. Analysis of intrusion detection techniques in cloud computing

References	Features					
	Detection technique	IDS type	Positioning	Detection time	Data source	Attacks covered
[14]	Signature based	Revocable identity based (RBS)	Cloud server	Real time	Network traffic, Signature of known attack	Existential forgery on adaptively chosen messages and identity attacks in the random oracle model
[15]	Signature based	Network based	Each cloud region	Real time	Virtual network layer of cloud	Distributed attacks at cluster or cloud layer
[16]	Signature based	Network based	At each node of cloud	Real time	Network Traffic, cloud-based signature learning service	Signature attack on cloud
[17]	Signature based	Network based	Each cluster of cloud	Real time	Network Traffic, real-world IDS traces	Detection of zero day attack
[18]	Signature based	Network based, host based	Different parts of the cloud	Real time	Network traffic	Detection of distributed attacks
[19]	Anomaly based detection	Network based, host based	Different parts of the cloud	Real time	Network traffic	Random attack in networks
[20]	Anomaly based detection	Host based	Public cloud environments	Real time	Host traffic	Dos attack on IAAS
[21]	Anomaly based detection	Network based	Different parts of the cloud	Real time	Network traffic	Mis-training of an IDS trained online
[22]	Anomaly based detection	Network based, host based	Intrusion detection system	Real time	Network Traffic, context awareness and cyber DNA	Cyber attack
[23]	Artificial based detection	Network based	Cloud region	Real time	Network communication	Trigger attacks
[24]	Artificial based detection	Neural network based	Cloud platform	Real time	Network traffic, KDD dataset	ANN based attacks
[25]	Fuzzy based detection	Network based	On cloud system	Real time	Normal and abnormal network traffic	Detection of zero day attack

(*continued*)

Table 7. (*continued*)

References	Features					
	Detection technique	IDS type	Positioning	Detection time	Data source	Attacks covered
[26]	Fuzzy based detection	Network based	Fuzzy-Logic engine based on IDSs	Real time	Network traffic	Cyber attacks
[27]	Fuzzy based detection	Network based	Different cloud computing platform	Real time	Cloud traffic	Cloud computing attacks
[28]	Genetic based detection	Network based	Cloud computing platform	Real time	Network traffic	Management, conservation and distribution of mutant rice seeds inventory
[30]	Genetic based detection	Cloud networks	Cloud computing platform	Real time	Cloud traffic	Different types of attacks on IDS
[31]	SVM based detection	Cloud networks	Different parts of the cloud network	Real time	Cloud traffic	ICMP Flood, Ping-of-Death, UDP Flood, TCP SYN Flood
[32]	SVM based detection	Network based	Cloud computing environment	Real time	Network Traffic	False positive rates

4.8 Hybrid Techniques

Hybrid techniques combine various such technologies together for a better result in sense of intrusion detection. This is such a kind of technology, which contains various flavours related to other techniques. NeGPAIM is based on hybrid technique combining two low level components including fuzzy logic for misuse detection and neural networks for anomaly detection, and one high level component which is a central engine analyzing outcome of two low level components. This is an effective model and does not require dynamic update of rules. It is more suitable to be integrated with soft computing techniques, which are traditional ones or focused towards intrusion detection.

With pros and cons of every technique, this is also not an exception. Some of the limitations under this technique are mainly oriented towards training profiles, period and rules. The lead role in this technique is of algorithm, which makes it stand clear form other techniques. Justin et al. [34] proposed a hybrid IDS model that uses SVM classifier for getting highly accurate results and anomaly-based detection is used for detecting DoS attacks in Mobile Ad-Hoc Networks (MANETs). Now, the analytical study of all techniques are shown in tabular format i.e. in Table 7. The table covers the comparison between different detection techniques based on certain silent features such as IDS type, Positioning, detection time, data source and attacks covered etc. Each detection technique has different positioning, detection time, data source and attack that effects the cloud-computing environment because network traffic, signatures, servers and cloud regions are different for each detection technique.

5 Conclusion

In this paper, different types of intrusion detection systems have shown that are useful in the cloud-computing environment. In the first section, we talk about different attacks on cloud platforms like Insider attack, Flooding attack, Port Scanning and attacks on VMs. After that a little description about firewall is given. Then we described different cloud based IDS techniques. The paper also covers different researches in tabular form that are helpful for understanding the cloud-computing scenario in efficient way. Furthermore, the analysis of different IDS techniques such as signature based, anomaly based, artificial based and genetic based detection etc. have been shown in the paper. The confidentiality, integrity, and availability of data in cloud that are affected by the intrusions are also presented here. Finally, the analytical study of all cloud based IDS techniques is done on the basis of salient features such as IDS type, positioning, detection time, data source and attacks covered. Each detection technique has different positioning, detection time, data source and attack that effects the cloud computing environment because network traffic, signatures, server positioning and cloud regions are different for each technique. With this analytical study, we presented a detailed analysis on how different IDS techniques have been used over the cloud platform and how we can better select the IDS based on our requirements.

References

1. Modi, C., Patel, D., Borisaniya, B., Patel, H.: A survey of intrusion detection techniques in cloud. J. Netw. Comput. Appl. **36**, 42–57 (2013)
2. Almorsy, M., Grundy, J., Ibrahim, A.S.: Adaptable, model-driven security engineering for SaaS cloud-based applications. Automated Software Engineering **21**(2), 187–224 (2014)
3. Du, Y., Zhang, R., Li, M.: Research on a security mechanism for cloud computing based on virtualization. Telecommun. Syst. **53**, 19–24 (2013)
4. Edurado, F.B., Monge, R., Hashizume, K.: Building a security reference architecture for cloud systems. Requir. Eng. **21**, 1–25 (2015)
5. He, J., Dong, M., Ota, K., Fan, M., Wang, G.: NetSecCC: a scalable and fault tolerant architecture for cloud computing security. Peer-to-Peer Netw. Appl. **9**, 1–15 (2014)
6. Hu, P., Sung, C.W., Ho, S., Chan, T.H.: Optimal coding and allocation for perfect secrecy in multiple clouds. Inf. Forensics Secur. **11**, 388–399 (2014)
7. Lee, J., Cho, J., Seo, J., Shon, T., Won, D.: A novel approach to analyzing for detecting malicious network activity using a cloud computing testbed. Mob. Netw. Appl. **18**, 122–128 (2012)
8. Li, J., Li, Y.K., Chen, X., Lee, P.P.C., Lou, W.: A hybrid cloud approach for secure authorized deduplication. IEEE Trans. Parallel Distrib. Syst. **26**, 1206–1216 (2014)

9. Rahat, M., Shibli, M.A., Niazi, M.A.: Cloud identity management security issues and solutions: a taxonomy. Complex Adapt. Syst. Model. **2**, 1–37 (2014)
10. Rho, S., Chang, H., Kim, S., Lee, Y.S.: An efficient peer-to-peer distributed scheduling for cloud and grid computing. Peer-to-Peer Netw. Appl. **8**, 863–871 (2014)
11. Li, Q., Han, Q., Sun, L.: Collaborative recognition of queuing behavior on mobile phones. Mob. Comput. **15**, 60–73 (2014)
12. Tak, G.K., Badge, N., Manwatkar, P., Rangnathan, A., Tapaswi, S.: Asynchronous anti phishing image captcha approach towards phishing. In: International Conference on Future Computer and Communication, vol. 3, pp. 694–698. IEEE (2010)
13. Malhotra, K., Gardner, S., Patz, R.: Implementation of elliptic-curve cryptography on mobile healthcare devices. IEEE (2007)
14. Jia, X., et al.: Efficient revocable id-based signature with cloud revocation server. IEEE Access **5**, 2945–2954 (2017)
15. Arjunan, K., Modi, C.N.: An enhanced intrusion detection framework for securing network layer of cloud computing. In: Asia Security and Privacy (ISEASP), 2017 ISEA. IEEE (2017)
16. Hamdi, O., Mbaye, M., Krief, F.: A cloud-based architecture for network attack signature learning. In: 2015 7th International Conference on New Technologies, Mobility and Security (NTMS). IEEE (2015)
17. Huang, S.-Y., Huang, Y., Suri, N.: Event pattern discovery on IDS traces of cloud services. In: 2014 IEEE Fourth International Conference on Big Data and Cloud Computing (BdCloud). IEEE (2014)
18. Mehmood, Y., et al.: Intrusion detection system in cloud computing: challenges and opportunities. In: 2013 2nd National Conference on Information Assurance (NCIA). IEEE (2013)
19. Kumawat, S., Sharma, A.K., Kumawat, A.: Intrusion detection and prevention system using K-learning classification in cloud. In: 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom). IEEE (2016)
20. Alarifi, S.S., Wolthusen, S.D.: Detecting anomalies in IaaS environments through virtual machine host system call analysis. In: 2012 International Conference for Internet Technology and Secured Transactions. IEEE (2012)
21. Fellin, C., Haney, M.: Preventing the mistraining of anomaly-based IDSs through ensemble systems. In: 2014 IEEE World Congress on Services (SERVICES). IEEE (2014)
22. Pan, Z., Pacheco, J., Hariri, S.: Anomaly behavior analysis for building automation systems. In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA). IEEE (2016)
23. Gupta, D., Gupta, S.: An efficient approach of trigger mechanism through IDS in cloud computing. In: 2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON). IEEE (2017)
24. Li, Z., Sun, W., Wang, L.: A neural network based distributed intrusion detection system on cloud platform. In: 2012 IEEE 2nd International Conference on Cloud Computing and Intelligent Systems (CCIS), vol. 1. IEEE (2012)
25. Alqahtani, S.M., John, R.: A comparative analysis of different classification techniques for cloud intrusion detection systems' alerts and fuzzy classifiers. In: 2017 Computing Conference. IEEE (2017)
26. Alqahtani, S.M., John, R.: A comparative study of different fuzzy classifiers for cloud intrusion detection systems' alerts. In: 2016 IEEE Symposium Series on Computational Intelligence (SSCI). IEEE (2016)
27. Sule, M.-J., et al.: Fuzzy logic approach to modelling trust in cloud computing. IET Cyber-Phys. Syst. Theory Appl. **2**(2), 84–89 (2017)

28. Kumar, R., Lal, S.P., Sharma, A.: Detecting denial of service attacks in the cloud. In: 2016 IEEE 14th International Conference on Dependable, Autonomic and Secure Computing, 14th International Conference on Pervasive Intelligence and Computing, 2nd International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech). IEEE (2016)
29. Mukkavilli, S.K., Shetty, S.: Mining concept drifting network traffic in cloud computing environments. In: Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid 2012). IEEE Computer Society (2012)
30. Raja, M.C., Rabbani, M.M.A.: Combined analysis of support vector machine and principle component analysis for IDS. In: International Conference on Communication and Electronics Systems (ICCES). IEEE (2016)
31. Fan, M.-J., et al.: TTRSIS: a cloud computing platform for rice functional genomics research through a reverse genetics approach. In: 2011 IEEE 11th International Conference on Bioinformatics and Bioengineering (BIBE). IEEE (2011)
32. Kannan, A., et al.: Genetic algorithm based feature selection algorithm for effective intrusion detection in cloud networks. In: Data Mining Workshops (ICDMW). IEEE (2012)
33. Yin, H., Gai, K., Wang, Z.: A classification algorithm based on ensemble feature selections for imbalanced-class dataset. In: IEEE International Conference on High Performance and Smart Computing (HPSC), 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), and IEEE International Conference on Intelligent Data and Security (IDS). IEEE (2016)
34. Justin, V., Marathe, N., Dongre, N.: Hybrid IDS using SVM classifier for detecting DoS attack in MANET application. In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 775–778. IEEE (2017)