State of the Art Intrusion Detection System for Cloud Computing

Azuan Ahmad[1], Wan Shafiuddin Zainudin[2], Mohd Nazri Kama[3], Norbik Bashah Idris[4], Madihah Mohd Saudi[1], Nur Hafiza Zakaria[1]

[1]Faculty of Science and Technology, Universiti Sains Islam Malaysia, Nilai, Negeri Sembilan, Malaysia
[2]CyberSecurity Malaysia, Malaysia
[3]Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia
[4]Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Malaysia

Abstract: The term Cloud computing is not new anymore in computing technology. This form of computing technology previously considered only as marketing term, but today Cloud computing not only provides innovative improvements in resource utilisation but it also creates a new opportunity in data protection mechanisms where the advancement of intrusion detection technologies are blooming rapidly. From the perspective of security, Cloud computing also introduces concerns about data protection and intrusion detection mechanism. This paper surveys, explores and informs researchers about the latest developed Cloud Intrusion Detection Systems by providing a comprehensive taxonomy and investigating possible solutions to detect intrusions in cloud computing systems. As a result, we provide a comprehensive review of Cloud Intrusion Detection System research, while highlighting the specific properties of Cloud Intrusion Detection System. We also present taxonomy on the key issues in Cloud Intrusion Detection System area and discuss the different approaches taken to solve the issues. We conclude the paper with a critical analysis of challenges that have not fully solved.

Keywords: Cloud Computing, Intrusion Detection System, Virtual Machine, Grid Computing, Artificial Immune System.

1. Introduction

There are problems with the implementation of Cloud computing systems that will be as a basis in this paper. Cloud computing is the new concept of computing where people only need to pay for services and resources without needed to place any cost for physical hardware. With the implementation of Cloud computing in the application today, it emerges a new technique in software development and deployment. It also changes how people are using and managing resources. Cloud computing can be defined as internet-based computing, where shared resource, software and information are provided to the user on demand [1].

Cloud computing systems are distributed and nesting a lot of resources and private information, therefore because of their nature, cloud computing environments are easy targets for intruders looking for possible vulnerabilities to exploit [2]. When organizations and companies which are using Cloud computing services, they will move their resources from their own private infrastructure to the Cloud infrastructure. If the Cloud is compromised, the organization’s resource will be at risk. Cloud Computing systems need protection mechanisms that will monitor the network activity and detect if any intrusion attempts happen within the Cloud Computing infrastructure whether it was from external or internal sources [3]. In fact, the cheap availability of significant amounts of computational resources can be regarded as a means for easily perpetrating distributed attacks, as it has recently been observed in several security incidents involving Amazon’s EC2 cloud infrastructure [4].

Cloud implementation introduces a new term, "co-residency" which means that multiple independent customer share the same physical infrastructure [5]. Hence, it was possible for different Cloud host residing in a single machine. There are several methods for neighbour discovery between Virtual Machine (VM) in a Cloud infrastructure; therefore, it is crucial to provide countermeasures for this type of attack. Ristenpart et al simulates the "co-residency" attack on Amazon EC2, which is one of the largest Cloud service providers [6]. Their works make use on freely available open source software. Inter VM's communication also become a big concern when we are implementing Cloud Computing system where communication between Clouds are not monitored and controlled. When implementing VM in the system layer of the Cloud, each Guest Operating system (OS) exposed to the risk of being attacked by other Guest OS either intentionally or accidentally. In a way to protect each Cloud, a new method is required to monitor inter VM's activity and detect if any abnormalities occur and at the same time to block the events from occurring [7].

In addition, there are lack of specific IDS built to protect Cloud computing systems [8]. Current implementation of IDS in the Cloud computing systems are still using the traditional way which installing traditional open source or enterprise IDS in the Cloud Computing server to protect the Cloud Computing systems. These traditional IDS implementation, such as on virtual machines (VM), which is considered more vulnerable with diverse security requirements [9]. Implementing traditional IDS need a lot of self-maintenance and did not scale with the customer security requirements. In addition, maintenance of traditional IDS in Cloud Computing system requires expertise and consume more time where not each Cloud user have [10, 11]. An attack against a cloud computing system can be silent for a network-based IDS deployed in its environment, because node communication is usually encrypted. Attacks can also be invisible to host-based IDSs, because cloud-specific attacks don’t necessarily leave traces in a node’s operating system, where the host-based IDS reside. In this way, traditional IDSs can’t appropriately identify suspicious activities in a cloud environment.

Worse come to worst, a decentralized traditional IDS approach where being implemented in current Cloud computing infrastructure will make the IDS management become more complicated [12]. Cloud subscribers that concern about their data protection will install their own IDS and this action will isolate the Cloud Service Provider (CSP) from the IDS management realm and CSP will have no authority in managing each Cloud subscribers' local IDS. This approach also affects the bill that Cloud subscribers will pay if the IDS were installed on their own host because monitoring intrusions may consume excessive amount of hidden data transfer [13]. Furthermore, each of the subscriber' IDS will not be the same in term of type and configurations and each user may have the risk of outdated signatures. If any attack happens and the IDS signature was outdated, the IDS will not treat the event the same way as IDS with updated signature and some of the IDS may cause a false negative detection. This will bring risk not only to the Cloud subscriber itself but also to the other Cloud users and in worst case scenario, this attack also may affect CSP and the whole system.

Cloud Computing is a new implementation of computer technology and open a new research area and create a lot of opportunity of exploration. One of the new implementation in Cloud is Intrusion Detection System (IDS). Cloud Computing is a Model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is based on five attributes: multi-tenancy (shared resources), massive scalability, elasticity, pay as you go and self-provisioning of resources.

The objective of this study is to characterise and provide a comprehensive review on the state of the art research in Cloud IDS. To the author's knowledge very few comprehensive studies on Cloud IDS have been conducted. For this purpose, a comprehensive review is conducted within this paper to discuss the state of the art research on Cloud IDS.

2. Motivation: the need for Cloud Intrusion Detection System

With respect to Cloud computing, to the best of our knowledge, we are the first to identify the intrusion detection problem for such systems based on artificial immune system (AIS). However, there have been efforts in traditional systems to address this problem. An obvious example of such systems is network intrusion detection system (NIDS) where an intrusion detection system is usually deployed at a border node to look after a whole network of computers. As part of the network, different sub-domains or clusters can have varying security requirements [14]. This NIDS implementation introduce a new Virtual Machine (VM) level threats in cloud computing because the existence of numerous VMs owned by different Cloud users significantly increases attack surface for cross-VM (or VM-to-VM) attacks [15].

Traditional IDS need a lot of self-maintenance and did not scale with the customer security requirements. In addition, maintenance of traditional IDS requires expertise and consume more time that normal company did not have [10, 11]. The cost of maintaining and installing the traditional IDS is also a big consideration in implementing IDS in an organization. In addition, a decentralized traditional IDS approach where being implemented in traditional IDS can increase the network vulnerabilities in the protected system when the IDS system is deployed and implemented together in the same network and made visible to others. The IDS itself are exposed to the internal attacks where attacker from the same network will have access to the IDS and launching attack directly towards the IDS. The IDS must be isolated and invisible from the same network where the host and servers reside [11].

To protect computing infrastructures which contains valuable assets from cyber-attacks, most enterprises set their strategy to deploy their IDS on dedicated hardware. However, such strategy is no longer effective today when small and medium enterprises (SMEs) are conveniently tapping into the Cloud environment which provides them the platform, infrastructure and software as services on a pay-per-use basis [9]. Moreover, IDS is commonly deployed in the traditional way, such as on virtual machines (VM), which is considered more vulnerable with diverse security requirements. In the traditional deployment, the benefits of customization and on-demand operations offered by Cloud are contradicted by the lengthy intrusion response time and thus affecting the overall security of the system [10].

2.1 Research on Cloud Computing Intrusion Detection System

This paper reviews the research related to the detection of intrusions for Cloud Computing in particular. Therefore, the existing literature in these domains has been explored to draw a comparative analysis of the proposed approach with the related works in Cloud Intrusion Detection. Fig.1 shows the scattered plot of the research that being investigated within this review. The plot was marked with numbers which indicated the reference number at the end of this paper.

2.1.1 Virtual Machine Introspection (VMI-based) and Grid Cloud IDS

The research related to Cloud IDS started since 2003 where Garfinkel .T and Rosenblum .M proposed the virtual machine introspection based architecture for intrusion detection [16]. At that time, normal implementation of cloud infrastructures includes the deployment of virtual machine monitors (VMM). Hence, this research also related to the research based on VMM. Virtual machine introspection (VMI) is the process of monitoring and inspecting a virtual machine from the outside for the purpose of analysing the software running inside it [17]. As explained in their paper, VMI IDS will monitor cloud client directly by using command namely Inspection Command to monitor VM state, Monitor Commands to monitor VM event and Administrative Commands to control the execution of a VM. This host-based IDS (HIDS) make a decision based on the Operating System (OS) Interface Library and Policy Engine. The prototype, Livewire will suspend the execution of the VM until the administrator responds to that event. This procedure may bring a concern when the VM operation suspended and user is unable to access the VM. This may affect the availability of the Cloud guest system. The experiment conducted using custom attacks that launch at the monitored host. The results show that Livewire are able to detect all the attacks. From the author point of view, this implementation is successful but may need some improvement in term of resource management especially if this system is implemented in cloud environment.

A few years later Roschke et al proposed a VM compatible IDS architecture in their paper Intrusion Detection in the Cloud [18]. This research provides a solution to protect Cloud environment by placing the IDS at each VM nodes. The NIDS rely on the detection of the signature-based IDS that analysed and detect any intrusions targeting the Cloud. At the same time, AV. Dastjerdi et al proposed mobile agent implementations in Cloud computing environment where the IDS located at every VM host [19]. The proposed system based on anomaly detection engine where it provides IDS for Cloud application regardless by their location. The issue with their proposed system is the implementation will produce network load with the increase of VMs attached to mobile agent.

K. Viera et al also proposed a solution in protecting Cloud in general but more focused on Grid computing implementation [3]. The proposed hybrid system integrates knowledge and behaviour analysis together to detect specific intrusions and placed on each node of the grid system. Each IDS node cooperatively takes part in intrusion detections and once any attacks were detected, they will broadcast the alert among them using middleware communication mechanism. The experiments were conducted with a prototype that they developed to evaluate the proposed architecture using Grid-M [20]. Grid-M is a middleware for simulating mobile device, sensor and grid computing developed by a research group at the Federal University of Santa Catarina. The datasets were generated from audit elements coming from both the log system and from data captured during node communications. The results show that the proposed system generates low number of false positives, but after several repetitions, the quantity of false positives varied and uncertain. However, this system provides low processing cost while still providing a satisfactory performance for real-time implementation.

Work by S Gupta et al provided a solution if detecting insider attacks or inter-VM attacks by detecting malicious system call sequences of well-known program [21]. Their proposed system will grab the fingerprint of the well-known program and monitor the system call activities during execution. The detections are based on the stored system call array and if the execution did not execute the next expected system call, the event will be considered malicious. From our point of view, developing the system calls fingerprint is a time-consuming task and the author still using manual technique which is not suitable in Cloud environment.

The recent work from P. Mishra et al proposed Cloud IDS based on VMI which having two major detection components; Traffic Monitoring for performing traffic analysis in detecting network based attack and Process Monitoring which does the process-monitoring at VMM-level without affecting any operations running on VMs [22]. They use three different datasets for experiment and the results shows a great performance result where 98.8% detection accuracy for UOC dataset [23], 98.9% accuracy for CAIDA [24] and 95.43% accuracy for UNSW-NB dataset [25]. Table 1 summarizes cloud IDS research on VMM technology that reviewed in this sub-section.

2.1.2 Distributed, Collaborative and Agent based Cloud IDS

Distributed Cloud IDS introduced by Irfan Gul and M. Hussain make use of multi-threading agent in monitoring and handling large amount of information in Cloud environment [26]. The agents then send the monitoring information to the third-party monitoring service for analysis and reporting any incidents. Their proposed system was tested with custom Denial of Service (DoS) attack targeting the Cloud network and the results show that the multi-threading system provides nearly 50% improvement of processing time compared to single-threading system. The same year, Cloud IDS described by ST. Zargar et al covers protection for two service level; Infrastructure level which provides a comprehensive hybrid Intrusion Detection and Prevention (IDP) system and virtual level where users are provided with software level IDP [27]. Within infrastructure level, the system cooperates with each other to create a comprehensive global version of all the clusters' databases on global infrastructure layer that is shared and used for detection and prevention among different cloud providers.

Some of the solutions focused on developing adaptive and distributed Cloud IDS. D Krishnan and M Chatterjee suggest that Cloud IDS can perform very well if the Cloud IDS can adapt to the environment and at the same time communicate with other IDS in different Cloud locations [28]. Their hybrid IDS which contains both anomaly and behaviour based detection will monitor Cloud environment and if any intrusions event occur, the IDS will distribute the alert to other IDS nodes so that each nodes update with the situations. IDS detection using behaviour based will monitor the current behaviour of the Cloud environment like number of users connected, log in time of users, bandwidth utilization, incoming and outgoing traffic flow, various connected ports, protocols and IP addresses used in incoming received requests and the detection engine will report if any deviation occurs compared to the recorded normal behaviour profile.

Nguyen Doan Man and Eui-Nam Huh proposed a collaborative intrusion detection system framework for protecting cloud computing environments. Their work consists of three main components; IDS Manager, which resides at the management region of a Collaborative Cloud, IDS Dispatcher, which is built inside each Cloud region, and Elementary Detector, which is distributed to monitor each VM and generates alarms for any detected intrusions [30]. The author did not provide any experiments and results from this research.

A similar work from P. Ghosh et al improves the model by generating Virtualised "Mini-IDS" for each Cloud host besides provides multi-threading monitoring and third party analysis service [29]. A mini IDS will be assigned for a specific Cloud host each time a new host is generated. Each instance supervises on each user activities and sends a report of all the activities to the IDS Controller via cloud NIDS after the end of each session. The proposed system will be able to handle large network traffic from Cloud users and provides security at the same time. The work of K.M.M. Vieira et al proposed a new approach to combine autonomous system and machine learning [30]. In their work, the autonomous system is following Monitor-Analyse-Plan-Knowledge (MAPE-K) cycle composed by the monitoring, analysis, planning and executing modules. They used sensors for collecting data from IDS logs, network traffic, system logs, and data communication. They also make use of Apache Hadoop for storage and analytics.

I. Jeganathan and A. Prakasam proposed agent-based Cloud intrusion detection system that monitoring and analysing clients' network packet at the same time filter the illegal user from accessing the cloud environment [31]. The agents send intrusion alert to a monitoring service for further action. Their proposed system will be placed outside the cloud environment where there are heavy network traffics such as switch, router or gateway for network traffic monitoring to have a global view of the system.

Araújo et al. proposed an elastic and internal Cloud-based detection system (EICIDS). This type of IDS is based on protection of virtual machines against internal users who can use some VMs to perform malicious activities which is part of our research [32]. Monitoring of virtual machines is done by IDS sensors dispersed in the cloud environment, and the instantiation of these sensors is made in each VM, where the packets passing in VMs are captured and subsequently analysed for the identification of threats. Thus, the entire virtual environment is monitored, while the remaining components of EICIDS reside outside the virtual environment are thus protected from possible attacks by compromised VMs. However, the architecture of EICIDS is centralised IDS admin and there is no signature generation system. Even this proposed system did not provide protection for outsider attacks.

In their research, Al Haddad et al proposed a collaborative network intrusion detection system for cloud computing environment. Their work proposed that the NIDS should be placed at the front end as well as at the back end on Virtual Machine Monitor (VMM) of a cloud network environment [33]. This hybrid-based NIDS consists of packet sniffing module, signature-based detection, anomaly detection, alert system and central log database. From author point of view, placing multiple NIDS inside a cloud network environment will result a complex configuration of a set of NIDS and the monitoring process will consume more resources than what we can imagine. The researcher still in the experiment phase and so far, no experimental results were provided.

Singh et al proposed a novel Collaborative IDS Framework for Cloud computing environment [34]. This framework integrates Snort to detect the known attacks using signature matching. To detect unknown attacks, anomaly detection system (ADS) is built using Decision Tree Classifier and Support Vector Machine (SVM). Alert Correlation and automatic signature generation reduce the impact of DoS and Distributed Denial of Service (DDoS) attacks and increase the performance and accuracy of IDS. However, it requires a high training time. Table 2 lists and analyses the distributive, collaborative and agent-based cloud IDS research based on their type, method, positioning, dataset, advantages and also their limitations.

2.1.3 IDS as a Service

There are some researchers provide different perspectives of Cloud IDS such as providing IDS as a Service. The work of Wang et al distributes IDS into local and remote components which local components collect and analyse logs in the client location while remote component focused on detecting intrusions based on the analysis from the local components [35]. W. Yassin et al suggests an alternative in intrusion detection where a framework of IDS based on Cloud was proposed [11]. The cloud-based IDS make use the Cloud technology for managing and detecting intrusions targeting a normal network environment. In detail, the IDS components such as User Database, Signature Database and Analysis Engine located in a Cloud environment, where the users' traffic are directed to the IDS through a secured Virtual Private Network (VPN) connection. The concerns about this implementation are internal attack may become invisible from the view of IDS and the VPN network is a single point of failure where any disruption of the connection will bring down the whole system. In addition, the increasing number of clients will increase the workload of the IDS Cloud. The same idea also shared in Hamad H. and Al-Hoby work on managing IDS as a service [36]. Their work tries to replace the traditional local server-based network environments with a cloud-based network infrastructure that monitor the network traffic and analyse for any intrusion attempt. This mechanism is offered to the end user as a service. In the proposed work, they utilise the huge performance of Cloud infrastructure for fast and efficient search algorithms. The proposed system able to receive the subscriptions requests from the cloud users and translates these requests into a standardised signature that can be deployed and utilised as the Cloud Intrusion Detection Service (CIDS). An experiment was conducted by using 500 signature definitions and the detection rate form the proposed system less than the traditional implementations. However, this system shows an improvement in term of detection overhead, compared to the traditional IDS implementation.

Still in the context of Cloud-based IDS perspective, one of the concerns in this type of implementation is the IDS became the victim of the attack itself. By considering this issue, HA Kholidy and F Baiardi proposed Cloud-based Intrusion Detection system (CIDS) which applied scalable and elastic architecture with point-to-point (P2P) solution and no central coordinator, which means they try to eliminate single point of failure [37]. Their proposed system distributes the workload of a single IDS into several cloud locations and isolates the task using monitored VM. This hybrid IDS claim that it can detect the masqueraders that access from several nodes and both host-based and network-based attacks because they are monitoring any intrusion in the middleware layer of a cloud. Based on CIDS, the same author proposed the enhanced version of their works named Hierarchical and Autonomous IDS for Cloud Systems (HA-CIDS) [38]. In this model, their IDS not only detect masquerades attack, but the detection also covers DDoS, host based and network-based attack with the inclusion of OSSEC HIDS, Snort NIDS and integrity checker within their detection mechanism. The detection mechanism is not distributed as previous model but located in a single cloud node.

The recent work by Azuan et al provides a Danger Theory Model Cloud-based IDS. This is the only work that using Artificial Immune System (AIS) for Cloud-based IDS, namely SaaSIDS [39]. SaaSIDS is a Cloud host that receive network traffic and analysing them for intrusion detections via hybrid engine which provides signature-based and anomaly detections. The system consists of three major components; SaaSIDS sensor, a sensor that installed on users' network and forward the packet through VPN to the SaaSIDS cloud. The other component is SaaSIDS Service Component which filter network traffic and pre-processing them before analyse it is using Hybrid Detection Engine for intrusion detections.

The problem of traffic bottlenecking is the main issue for IDS as a Service model. The work of S Garg and K Kaur provides a solution for this problem by maintaining a group of IDS as a Service and load balancing them to support a heavy traffic of clients' network data [26]. The signature-based IDS use Snort NIDS for intrusion detection. From the experiment, their proposed model able to eliminate single point of failure by introducing concept of multiple IDS in cloud environment and increase availability of IDS service for cloud users by balancing load between IDSs.

Recent work from SM Alqahtani et al proposed a Cloud-based IDS for detecting DDoS attack [36]. They proposed that the IDS placed in a separate VM and dedicated for analysing intrusion data. Another VM was created for monitoring and sending suspicious packet to the IDS. From the experiment, the processing required for detecting ICMP Flood attack is 39-40%. Their system is able to provide promising performance improvement compared to traditional method.

Single point of failure is the main concern of IDS as a Service architecture. The work of M. Mbaye and C. Ba proposed distributed Cloud-based IDS with the Publish and Subscribe paradigm [41]. They considered client as a Publisher which sent intrusion data to the IDS while the IDS as a Subscriber which receive the intrusion data together with the taxonomy of the intrusion. The distributed IDS will receive the data based on the taxonomy which each IDS will support different kind of taxonomy. In a simple view, table 3 describes Cloud IDS as a Service research in tabular form.

2.1.4 Open Source Cloud IDS

Open source software is the best cost-effective solutions in solving real world problems and at the same time did not sacrifice the performance. Mazzariello et al in their research provides a solution for detecting intrusions by using network intrusion detection system (NIDS) for Open Source Cloud Computing environment [42]. In the paper, they provide a review on eucalyptus, an open source cloud management system and deploying a signature-based IDS inside the eucalyptus environment. They try to prove that a carefully deployed traditional solution could mitigate a severe problem in cloud computing environment. In the implementation, they install IDS at the frontend of the cloud environment. Such implementation has a flaw where it tends to make inter-cloud attacks invisible from detection. The author did not provide any IDS performance result based on detection rate.

B Borisaniya et al proposed a solution in Cloud IDS by implementing open source technology in developing their prototype [43]. They choose to use Eucalyptus for the Cloud framework and Snort as the NIDS that located in each Cluster Controller (CC) to monitor network traffic. From their perspective, this approach allows the Cloud administrator to monitor the type and source of the attack, which in turn can be used to prevent the similar future attacks. They employ Honeypot in detecting unknown attacks since honeypot will monitor for suspicious behaviour. The experiment shows that the proposed system able to detect medium and low level of security threats and still need some improvement in detecting high level of security threat.

HM Alsafi and WM Abduallah proposed a Cloud IDS that focused on Infrastructure as a Service (IaaS) layer of Cloud environment and implementing hybrid detection mechanism which combine anomaly and signature based detection [44]. Further than just detect and reporting intrusion, their proposed system includes the protection mechanism which terminates the user session that is being used for the attack, block access to the target from the offending source and block all access to the targeted host, service, application, or other resource.

More recent work that take the benefits of honeypot in protecting Cloud environment also been done by AA Thu which [45]. The proposed system placed honeypot within the Cloud environment to monitor any internal attacks that targeted the other Cloud host. The honeypot will work closely with IDPS in protecting the Cloud infrastructure. From the testing, the result shows that IDPS system with honeypot works better than traditional implementation of IDPS.

The work of T Xing et al also implemented open source technology in their proposed system, SnortFlow [46]. SnortFlow is the combination of Snort, an open source NIDS and OpenFlow, communications protocol that gives access to the forwarding plane of a network switch or router over the network. The proposed system has multiple module including SnortFlow Server which evaluates the network security status and generates actions to be pushed into the controller, SnortFlow daemon for collecting alert data from Snort agent in Dom 0 and Alert Interpreter, takes care of parsing the alert and targets the suspect traffic. The experiments are conducted to find the best place for implementing SnortFlow. From the result, the SnortFlow perform more efficient when implemented in the Domain 0. The work from T Kuldeep et al also proposed the usage of Snort NIDS in their implementations. They proposed the location of Snort NIDS is behind the gateway which monitors all the traffic going through the network gateway [47]. JK Khatri and G Khilari on the other hand proposed the Cloud IDS by using Kernel-based Virtual Machine (KVM) and Suricata NIDS [48]. Both open source applications were installed on Ubuntu Linux. Recent work from Priyanka Sharma et al provides Cloud environment using VirtualBox open source virtualisation software and OpenStack Cloud environment framework [49]. They launched DoS attack targeting their Cloud and the result shows that OpenStack take longer time to load an image compared during normal situation.

There is an implementation where multiple open source applications are combine and work closely in protecting Cloud from threats. The work from C Ambikavathi and SK Srivatsa make use OpenNebula as the Cloud computing platform, Snort as the signature -based NIDS, Bro also as signature-based NIDS and OSSEC open source signature-based HIDS [50]. The aim of the author is to provide total protection mechanisms by implementing all the available open source applications. The same work also proposed by W. Muche where they integrate the use of Snort for NIDS, OSSEC for HIDS and expand the capability of anomaly detection by using Naïve Bayes Tree (NBTree) classifier [51]. By using KDD'99 dataset, their work was able to achieve 95.5% detection. Table 4 listed the Cloud IDS research based on open source approaches.

2.1.5 Machine Learning Cloud IDS

Make use data mining and machine learning algorithm for classifying intrusions is also being adapted by several researchers. G. Sathya and K Vasanthraj proposed a work based on data mining technique [37]. In their work make use of C4.5 algorithm in detecting anomaly attacks. In their multi-level IDS for Cloud computing, they monitored network traffic and identified the attack at the first level. The second level classifies the attack into four categories and the third level identifies the type of the attack. More recent work by M Moorthy and M Rajeswari focused on using Genetic Algorithm (GA) in generating new rules in their proposed cloud Intrusion detection system [53]. Their work generate the network profile based on CIDD [37] by analysing real-traces in the dataset. Their proposed system can achieve 80% of True Positive Rate (TPR) during the experiment.

Machine learning algorithm also implemented in the work of MN Ismail et al. They proposed an IDS for detecting flooding based DoS attack targeting Cloud network by using covariance matrix approach [54]. The experiment is done in two phases; Training phase where the IDS were run with the normal network traffic and Testing phase where the IDS were run with the abnormal network traffic which contains flooding attacks. From the experiment they prove that there is a huge different between normal network traffic and network traffic under flooding-based DoS attack by using covariance matrix.

The latest work from HA. Kholidy et al implemented finite state Hidden Markov Model (HMM) in predicting multi stage attack in Cloud computing environments [55]. They include HMM as an improvement from their previous work in [38] for predicting and provides early warning for any future attacks. Their proposed system works by tracking the evolution of an attack while it is in progress, the state changes and the system can trigger appropriate responses based on a confidence level threshold, which would result in a lower false positive rate. The proposed prediction model has successfully fired the early warning alerts before the launching of the LLDDoS1.0 attack by 39 minutes plus 37 seconds and 64 minutes plus 42 seconds before the detection phase starts.

J. Arshad et al. proposed an intrusion severity analysis for cloud computing where in their research, they used the hybrid approach where the attacks were detected based on the attack database that they provide and from the Profile Engine (PE) which is based on the behaviour of the monitored virtual machines (VM). This machine learning based IDS using classification technique for intrusion severity analysis from the monitored system calls. The dataset used in this research is the artificial data generated from the computer program. This dataset did not provide the real cloud environment and did not represent the actual response of a cloud environment towards any attack [14]. The results obtained from the research successfully demonstrate the effectiveness of the intrusion severity analysis method for Clouds but the dataset and may be questionable because the research used the self-generated dataset and they did not provide details about the methodology in building their datasets.

In the same year, work from U Hameed et al using Genetic Algorithm (GA) in detecting intrusions in Cloud computing environment especially in SaaS model [56]. Their proposed genetic algorithm engine analysed data and matched the data with the signature database in the detection engine. This system checks the intrusions by matching the signature in knowledge base. If the location is not matched with any existing details in the knowledge base it provides an exit from the system. If existence check is passed it analyse and matches the data for the proper recognition based on the fitness function X=δX0. If the fitness is proven, then different authentication checks are implemented to reach the result at each step it applies genetic algorithm. If the desired record is not matched it reproduces the new record by mutation, performs fitness test X=δX0 and rechecks from the data in knowledge base. Same method will be repeated for three generations as per termination criteria.

The same algorithm also sparks the inspiration for P Singh and B Hazela to propose a Cloud IDS model based on GA [57]. GA's aim is to produce the best solutions by the evolution of a sample set of potential solutions [58]. Inside the sample set, solutions that are poor tend to die out while the better solutions mate and propagate their advantageous traits, thus introducing more solutions into the set that boast better potential. Their proposed work is the mix of Cloud Intrusion Detection System and two types of chromosomes based on different criteria which is based on the job length and bandwidth utilisation of the resources. Based on the selected criteria, the system performs the crossover operation with the aid of neural network. The result will be the best chromosome of the first generation. From the experiment, the proposed model able to detect 57% of random sets of cloud attacks.

JK Seth and S Chandra come with a proposal that provides Cloud protection based on the user risk level [59]. They believe that every cloud user did not require the same security level of protection. In their proposed work, they classify the user risk level into four categories; normal, low, medium and high, based upon stored rules and pattern and this process will use Artificial Neural Network (ANN) classification algorithm. The repository will update the rules on occurrence of new pattern and train the classifier at the time of minimal load on cloud. The proposed model increases resource availability and optimise IDS resource utilisation.

Deshpande et al in their research proposed a HIDS for cloud computing environment based on system call trace analysis where only the failed system call were used to predict the intrusion [60]. The proposed system makes use of k-nearest neighbour (kNN) algorithm for comparing the current information with the available database. The prototype developed based on four main modules; Data Logging Module, Pre-processing Module, Analysis and decision engine and Management Module. Based on the paper, the experiment was conducted using a list of self-generated system calls based on Linux API. The result has been estimated using three different real-time datasets, with a time window of 30 and 60 s. From the paper the prototype can achieve the accuracy with a high sensitivity of 96%.

As discussed in the previous section, "co-residency attack" is a current threat in Cloud computing environment. N Pitropakis and C Lambrinoudakis support this statement by providing a solution for detecting this type of attack by using Smith-Waterman algorithm [61]. In their latest work, they make use of Graphical Processing Unit (GPU) processing in supporting the huge and complex calculation related to Cloud. GPU processing may improve the overhead processing of Cloud IDS in analysing and detecting intrusion from a large amount of data. From the experiment, they found that using GPU parallel processing achieved six times faster performance compared to normal Central Processing Unit (CPU) processing.

In computer networking, port mirroring is the method to duplicate all port in the network device towards a single port. NS Aljurayban and A Emam implement port mirroring method in collecting network traffic in the Cloud environment and analyse the traffic using Artificial Neural Network (ANN) algorithm [62]. From the experiment they got great result of sensitivity with a good result in accuracy. Extending the work of previous research, GK Chaturvedi et al combine Fuzzy-Clustering with Artificial Neural Network in providing a better intrusion detection model for Cloud Computing [63]. The dataset is divided into two groups which are training and testing. Their proposed work divides the training data into several subsets using fuzzy clustering technique while at the same time trains the different ANN using different subsets. Then their model will determine membership grades of these subsets and combines them via a new ANN to get final results.

In their paper, Kwon .H et al proposed a self-similarity based lightweight intrusion detection method as a solution for protecting cloud environment. They used Cosine Similarity Based Self-similarity as a detection algorithm and during the experiment, they monitored Windows event log from the DARPA 1999 datasets for any intrusion based on Security ID (SID) and EventID [64]. In this experiment, the overall false-positive ratio was 4.17 %. They claim that their IDS can work robustly even though the Windows event log does not include enough information regarding security rather than the other operating system’s audit log.

Recently, game theory has been used extensively to model and analyse network security issues. Game theory is a machine learning approach that provides a set analytical and mathematical framework to model rational decision-making or strategies of multiple players having different objectives interacting with each other [65]. The proposed work from Z. Li et al provides a protection for Cloud from intrusions by using differential game model [66]. The simulation results show the changes in the probability under the optimal strategies condition. Using the game theoretic framework, dynamic optimal strategies can improve the security of cloud computing system and energy consumption in the proposed optimal strategy is significantly lower than the static strategy.

Artificial Immune System (AIS) is one of the solutions that try to mimic our body protection against pathogen. This is because our body protection system always accurate and less prone to fails and this is become the main reason why AIS will provide the same result. One of AIS method, namely Dendritic Cell Algorithm (DCA) was inspired by one of our body cell type that monitored the body tissue for any pathogen [67]. This algorithm activated by multiple signals for calculating the maturity of the monitored environment where the matured Dendritic Cell (DC) indicates the malicious level of the environment and on the other hand, semi-mature DC indicates the normal environment. The work from Azuan et al, using DCA for detecting intrusions attempt that targeting Cloud environment [68]. Their integrated system monitored Cloud infrastructure from the agents that installed on each Cloud VM and from virtual switch level where the "co-residency" attack could be detected. Each agent and virtual switch collect numbers of specific data recognised as signals value in DCA. The signals value then being normalised and analysed for the results between mature or semi-mature conditions. Table 5 provides a summary of Cloud IDS research in machine learning approaches.

3. Challenges

Based on the related literature, we found that the following issues have not been sufficiently solved. These are gaps in the reviewed work that would prove to be directions for future works. Table 6 shows a clear gap analysis that Cloud IDS research should fill especially in the following issues:

- Providing real Cloud IDS implementation: In identifying the performance and workability of a proposed Cloud IDS, prototypes need to be developed and tested in a physical Cloud computing environment. Most of the research provides solution and results based on simulation and static data analysis. Even some research that claim to be real implementation still provide analysis results based on static dataset and this is not really represents real Cloud IDS implementation. The real Cloud IDS must be developed based on a working prototype that monitoring Cloud network traffic or system calls or both which is termed as hybrid. Other research especially that implemented open source technology in developing Cloud IDS, more focused on making use of traditional methods in protecting Cloud environment. This framework did not really represent the state of the art Cloud IDS technology because implementing traditional method in Cloud computing environment will introduce another risk to the environment.
- Cloud subscribers' data privacy: Within the process of detecting intrusions involve monitoring enormous data flow and most of the data belong to subscribers and may contains sensitive or private information. As discussed in [69], protecting data privacy is the major challenges in Cloud computing and pooling user's data in Cloud introduces a new risk in data privacy breach.
- Detecting co-residency attack: [5] and [70] describe co-residency attack as an internal attack conducted by a tenant targeting another tenant residing within the same Cloud infrastructure. This type of attack is unique to Cloud and exist because of the nature of Cloud computing. Although this issue is important, little research has been carried out covering this challenge. Although multiple reviewed frameworks stressed on the importance for protecting Cloud from co-residency attack, very few of them implemented it. Other frameworks more focused on entry point security and endpoint security while neglecting the importance of monitoring the risk of co-residency attack.

4. Conclusions

Cloud IDS aims to provides protection for Cloud computing environment from attacks while maintaining its functionality. Protecting Cloud is importance since its nature that pool user data in centralised source [71]. We have given an extensive survey of current Cloud IDS research in this review which focused on different approaches in developing Cloud IDS frameworks. We also highlight the motivations for Cloud IDS and the basic definitions and principle of Cloud IDS in the literature.

Research in Cloud IDS is still expanding and there are areas of research to be explored especially with the current advancement of detection algorithm. As previously discussed where Cloud IDS research evolved from the Grid computing protection mechanism and current technologies make use of machine learning algorithm including game theory and Artificial Immune System (AIS). The future will explore the specific data set that represents Cloud computing environment which the analysis will describe true performance of Cloud IDS.

The future also may explore the detection of intrusions for big data that become the continuity of the Cloud computing research. [72] discussed that big data will become the future of Cloud research where data collected by Cloud become larger than any typical database may capture, stored and analyse. Future Cloud IDS framework need to be prepared for threat analysis related to big data.

References

[1] P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," *NIST special publication,* vol. 800, p. 145, 2011.

[2] S. Carlin and K. Curran, "Cloud computing security," 2011.

[3] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Intrusion detection for grid and cloud computing," *It Professional,* vol. 12, pp. 38-43, 2010.

[4] I. Federico, "Integrating a Network IDS into an Open Source Cloud Computing Environment," 2010.

[5] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Communications Surveys & Tutorials,* vol. 15, pp. 843-859, 2013.

[6] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in *Proceedings of the 16th ACM conference on Computer and communications security*, pp. 199-212, 2009.

[7] P. Cox. (2010). *Intrusion detection in a cloud computing environment*. Available: http://searchcloudcomputing.techtarget.com/tip/Intrusion-detection-in-a-cloud-computing-environment

[8] D.-G. Feng, M. Zhang, Y. Zhang, and Z. Xu, "Study on cloud computing security," *Journal of software,* vol. 22, pp. 71-83, 2011.

[9] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications,* vol. 34, pp. 1-11, 2011.

[10] I. Cymtec Systems. *Scout Cloud-Enabled IDS Fact Sheet*. Available: http://go.pardot.com/l/12332/2012-04-16/kjv2/12332/9341/Cymtec_Scout_IDS_Fact_Sheet_021412v2.pdf, 2012

[11] W. Yassin, N. Udzir, Z. Muda, A. Abdullah, and M. Abdullah, "A Cloud-based Intrusion Detection Service framework," in *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on*, pp. 213-218, 2012

[12] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," *Journal of Network and Computer Applications*, vol. 36, pp. 42-57, 2013.

[13] A. Greenberg, J. Hamilton, D. A. Maltz, and P. Patel, "The cost of a cloud: research problems in data center networks," *ACM SIGCOMM computer communication review*, vol. 39, pp. 68-73, 2008.

[14] J. Arshad, P. Townend, and J. Xu, "A novel intrusion severity analysis approach for Clouds," *Future Generation Computer Systems*, vol. 29, pp. 416-428, 2013.

[15] N. D. Man and E.-N. Huh, "A collaborative intrusion detection system framework for cloud computing," in *Proceedings of the International Conference on IT Convergence and Security 2011*, pp. 91-109, 2012.

[16] T. Garfinkel and M. Rosenblum, "A Virtual Machine Introspection Based Architecture for Intrusion Detection," in *NDSS*, pp. 191-206, 2003.

[17] K. Nance, B. Hay, and M. Bishop, "Virtual machine introspection," *IEEE Computer Society,* vol. 6, pp. 32-37, 2008.

[18] S. Roschke, F. Cheng, and C. Meinel, "Intrusion detection in the cloud," in *Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on*, pp. 729-734, 2009.

[19] A. V. Dastjerdi, K. A. Bakar, and S. G. H. Tabatabaei, "Distributed intrusion detection in clouds using mobile agents," in *Advanced Engineering Computing and Applications in Sciences, 2009. ADVCOMP'09. Third International Conference on*, pp. 175-180, 2009.

[20] H. A. Franke, F. L. Koch, C. O. Rolim, C. B. Westphall, and D. O. Balen, "Grid-m: Middleware to integrate mobile devices, sensors and grid computing," in *Wireless and Mobile Communications, 2007. ICWMC'07. Third International Conference on*, pp. 19-19, 2007.

[21] S. Gupta, P. Kumar, A. Sardana, and A. Abraham, "A fingerprinting system calls approach for intrusion detection in a cloud environment," in *Computational aspects of social networks (CASoN), 2012 fourth international conference on*, pp. 309-314, 2012.

[22] P. Mishra, E. S. Pilli, V. Varadharajant, and U. Tupakula, "NvCloudIDS: A security architecture to detect intrusions at network and virtualization layer in cloud environment," in *Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on*, pp. 56-62, 2016.

[23] D. Kirat, G. Vigna, and C. Kruegel, "BareCloud: Bare-metal Analysis-based Evasive Malware Detection," in *USENIX Security*, pp. 287-301, 2014.

[24] M. H. Bhuyan, D. Bhattacharyya, and J. K. Kalita, "An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection," *Pattern Recognition Letters,* vol. 51, pp. 1-7, 2015.

[25] N. Moustafa and J. Slay, "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," *Information Security Journal: A Global Perspective,* vol. 25, pp. 18-31, 2016.

[26] I. Gul and M. Hussain, "Distributed cloud intrusion detection model," *International Journal of Advanced Science and Technology,* vol. 34, p. 135, 2011.

[27] S. T. Zargar, H. Takabi, and J. B. Joshi, "DCDIDP: A distributed, collaborative, and data-driven intrusion detection and prevention framework for cloud computing environments," in *Collaborative computing: Networking, applications and worksharing (collaboratecom), 2011 7th international conference on*, pp. 332-341, 2011.

[28] D. Krishnan and M. Chatterjee, "An adaptive distributed intrusion detection system for cloud computing framework," in *International Conference on Security in Computer Networks and Distributed Systems*, pp. 466-473, 2012.

[29] P. Ghosh, R. Ghosh, and R. Dutta, "An alternative model of virtualization based intrusion detection system in cloud computing," *International Journal of Scientific & Technology Research,* vol. 3, pp. 199-203, 2014.

[30] K. M. Vieira, F. Schubert, G. A. Geronimo, R. de Souza Mendes, and C. B. Westphall, "Autonomic intrusion detection system in cloud computing with big data," in *Proceedings of the International Conference on Security and Management (SAM)*, p. 1, 2014.

[31] I. Jeganathan and A. Prakasam, "Secure the Cloud Computing Environment from Attackers using Intrusion Detection System," 2014.

[32] J. D. Araújo, D. de Andrade Rodrigues, L. S. de Melo, and Z. Abdelouahab, "EICIDS-elastic and internal cloud-based detection system," *International Journal of Communication Networks and Information Security,* vol. 7, p. 34, 2015.

[33] Z. Al Haddad, M. Hanoune, and A. Mamouni, "A Collaborative Network Intrusion Detection System (C-NIDS) in Cloud Computing," *International Journal of Communication Networks and Information Security,* vol. 8, p. 130, 2016.

[34] D. Singh, D. Patel, B. Borisaniya, and C. Modi, "Collaborative IDS Framework for Cloud," *International Journal of Network Security,* vol. 18, pp. 699-709, 2016.

[35] X. Wang, T.-l. Huang, and X.-y. Liu, "Research on the Intrusion detection mechanism based on cloud computing," in *Intelligent computing and integrated systems (ICISS), 2010 international conference on*, pp. 125-128, 2010.

[36] H. Hamad and M. Al-Hoby, "Managing intrusion detection as a service in cloud networks," *International Journal of Computer Applications,* vol. 41, 2012.

[37] H. A. Kholidy and F. Baiardi, "CIDS: A framework for intrusion detection in cloud systems," in *Information Technology: New Generations (ITNG), 2012 Ninth International Conference on*, pp. 379-385, 2012.

[38] H. A. Kholidy, A. Erradi, S. Abdelwahed, and F. Baiardi, "Ha-cids: A hierarchical and autonomous ids for cloud systems," in *Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on*, , pp. 179-184, 2013.

[39] A. Ahmad, B. Shanmugam, N. B. Idris, and G. N. Samy, "Danger Theory Based Hybrid Intrusion Detection Systems for Cloud Computing," *International Journal of Computer and Communication Engineering,* vol. 2, p. 650, 2013.

[40] S. Garg and K. Kaur, "Rules based Enhancement in Cloud Intrusion Detection System Service," *International Journal of Computer Applications,* vol. 72, 2013.

[41] M. Mbaye and C. Ba, "A distributed IDS Cloud service: an architecture based on Pub-Sub paradigm," in *Pages 225–235. 12th African Conference on Research in Computer Science and Applied Mathematics (CARI 2014)* , p. 376, 2014.

[42] C. Mazzariello, R. Bifulco, and R. Canonico, "Integrating a network ids into an open source cloud computing environment," in *Information Assurance and Security (IAS), 2010 Sixth International Conference on*, pp. 265-270, 2010.

[43] B. Borisaniya, A. Patel, D. R. Patel, and H. Patel, "Incorporating honeypot for intrusion detection in cloud infrastructure," in *IFIP International Conference on Trust Management*, pp. 84-96, 2012.

[44] H. M. Alsafi, W. M. Abduallah, and A.-S. K. Pathan, "IDPS: an integrated intrusion handling model for cloud computing environment," *International Journal of Computing & Information Technology (IJCIT),* vol. 4, pp. 1-16, 2012.

[45] A. A. Thu, "Integrated intrusion detection and prevention system with honeypot on cloud computing environment," *International Journal of Computer Applications,* vol. 67, 2013.

[46] T. Xing, D. Huang, L. Xu, C.-J. Chung, and P. Khatkar, "Snortflow: A openflow-based intrusion prevention system in cloud environment," in *Research and Educational Experiment Workshop (GREE), 2013 Second GENI*, pp. 89-92, 2013.

[47] T. Kuldeep, S. Tyagi, and A. Richa, "Overview-Snort Intrusion Detection System in Cloud Environment," 2014.

[48] J. K. Khatri and G. Khilari, "Advancement in Virtualization Based Intrusion Detection System in Cloud Environment," *International Journal of Science, Engineering and Technology Research (IJSETR),* vol. 4, 2015.

[49] P. Sharma, R. Sharma, E. S. Pilli, and A. K. Mishra, "A Detection Algorithm for DoS Attack in the Cloud Environment," in *Proceedings of the 8th Annual ACM India Conference*, pp. 107-110, 2015.

[50] C. Ambikavathi and S. Srivatsa, "Integrated Intrusion Detection Approach for Cloud Computing," *Indian Journal of Science and Technology,* vol. 9, 2016.

[51] E. W. Muche, "HYBRID INTRUSION DETECTION SYSTEM FOR PRIVATE CLOUD: AN INTEGRATED APPROACH," 2016.

[52] G. Sathya and K. Vasanthraj, "Network activity classification schema in IDS and log audit for cloud computing," in *Information Communication and Embedded Systems (ICICES), 2013 International Conference on,* pp. 502-506, 2013.

[53] M. Moorthy and M. Rajeswari, "Virtual Host based Intrusion Detection System for Cloud," *International Journal of Engineering & Technology,* pp. 0975-4024, 2013.

[54] M. N. Ismail, A. Aborujilah, S. Musa, and A. Shahzad, "Detecting flooding based DoS attack in cloud computing environment using covariance matrix approach," in *Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication*, , p. 36, 2013.

[55] H. A. Kholidy, A. Erradi, S. Abdelwahed, and A. Azab, "A finite state hidden markov model for predicting multistage attacks in cloud systems," in *Dependable, Autonomic and Secure Computing (DASC), 2014 IEEE 12th International Conference on*, pp. 14-19, 2014.

[56] U. Hameed, S. Naseem, F. Ahamd, T. Alyas, and W.-A. Khan, "Intrusion Detection and Prevention in Cloud Computing using Genetic Algorithm," *International Journal of Scientific & Engineering Research,* vol. 5, 2014.

[57] P. Singh and B. Hazela, "Design & Development of a new hybrid system to Prevent Intrusion at cloud using genetic algorithm," *International Journal,* vol. 4, 2016.

[58] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Infocom, 2010 proceedings ieee*, pp. 1-9, 2010.

[59] J. K. Seth and S. Chandra, "An Optimistic Approach for Intrusion Security in Cloud," *International Journal of Computer Applications,* vol. 97, 2014.

[60] P. Deshpande, S. Sharma, S. Peddoju, and S. Junaid, "HIDS: A host based intrusion detection system for cloud computing environment," *International Journal of System Assurance Engineering and Management,* pp. 1-10, 2014.

[61] N. Pitropakis, C. Lambrinoudakis, and D. Geneiatakis, "Till all are one: Towards a unified Cloud IDS," in *International Conference on Trust and Privacy in Digital Business*, pp. 136-149, 2015.

[62] N. S. Aljurayban and A. Emam, "Framework for cloud intrusion detection system service," in *Web Applications and Networking (WSWAN), 2015 2nd World Symposium on*, pp. 1-5, 2015.

[63] G. K. Chaturvedi, A. K. Chaturvedi, and V. R. More, "A study of Intrusion Detection System for Cloud Network Using FC-ANN Algorithm," 2016.

[64] H. Kwon, T. Kim, S. J. Yu, and H. K. Kim, "Self-similarity based lightweight intrusion detection method for cloud computing," in *Asian Conference on Intelligent Information and Database Systems*, pp. 353-362, 2011.

[65] T. Alpcan and T. Basar, "An intrusion detection game with limited observations," in *Proceedings of the 12th Int. Symp. on Dynamic Games and Applications*, 2006.

[66] Z. Li, H. Xu, and Y. Liu, "A differential game model of intrusion detection system in cloud computing," *International Journal of Distributed Sensor Networks,* vol. 13, p. 1550147716687995, 2017.

[67] J. Greensmith and U. Aickelin, "Dendritic cells for SYN scan detection," in *Proceedings of the 9th annual conference on Genetic and evolutionary computation*, , pp. 49-56, 2007.

[68] A. Ahmad, N. B. Idris, and M. N. Kama, "Cloud Intrusion Detection Model Inspired by Dendritic Cell Mechanism", International Journal of Communication Networks and Information Security (IJCNIS), vol. 9, No.1, 2017.

[69] Z. Wang, "Security and privacy issues within the Cloud Computing," in *Computational and Information Sciences (ICCIS), 2011 International Conference on*, pp. 175-178, 2011.

[70] Y. Zhang, A. Juels, A. Oprea, and M. K. Reiter, "Homealone: Co-residency detection in the cloud via side-channel analysis," in *Security and Privacy (SP), 2011 IEEE Symposium on*, , pp. 313-328, 2011.

[71] A. Al-Qerem1, A. Hamarsheh, "Statistical-Based Heuristic for Tasks Scheduling in Cloud Computing Environment", International Journal of Communication Networks and Information Security (IJCNIS), Vol. 10, No. 2, 2018.

[72] J. Manyika, M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, *et al.*, "Big data: The next frontier for innovation, competition, and productivity," 2011.

Table 1. Cloud Intrusion Detection System on Virtual Machine Monitor

Title	IDS Type	Detection Method	Positioning	Dataset	Advantages	Limitations
Livewire [16]	HIDS	Anomaly	On the hypervisor	Custom Dataset	Livewire are able to detect all the attacks in their experiment	Livewire will suspend the execution of the VM until the admin responds to that event
Intrusion Detection in the Cloud [18]	NIDS	Signature based detection	On each VM	Not stated	Secures VM based on user configuration.	Multiple instances of IDS are required which degrades performance.
IDS for Grid and Cloud Computing [3]	Hybrid	Anomaly based	On each Grid node	log system and from data captured during node communications	Low processing cost and satisfactory performance	Varied and uncertainty false positive results.
Fingerprinting system calls approach for IDS in Cloud[21]	HIDS	Signature-based	Domain 0	Custom Dataset	Detects malicious software by system call sequence	Time consuming tasks and the author still using manual technique
NvCloudIDS [22]	Hybrid	Hybrid	VMI based IDS	UOC, UNSW-NB and CAIDA	Provides high detection result	Attack on the hypervisor will bring down the whole system.

Table 2. Distributive, Collaborative and Agent-based Cloud IDS Research

Title	IDS Type	Detection Method	Positioning	Dataset	Advantages	Limitations
Distributed Cloud IDS [26]	NIDS	Signature-based	On Domain 0	Custom DOS attack	Improvement in term of processing time	May unable to detect inter-VM attack.
Adaptive Distributed IDS for Cloud Computing [28]	NIDS	Hybrid	Any nodes	No explanation	May detects both Network attacks and host attacks.	Communication among IDS nodes may create additional unwanted traffic for the Cloud network.
Collaborative intrusion detection [15]	Hybrid	Real Time	On each node	No explanation	May detects both Network attacks and host attacks.	Need more explanations about the experiments and analysis.
Mini-IDS [29]	NIDS	Signature-based	On each cloud host	No Implementation	Able to handle large network traffic	Did not detect unknown attacks
IRAS [30]	NIDS	Anomaly-based	Agent on each Cloud host	Not yet implemented	provide self-awareness, self-configuration and self-healing in the cloud.	Single point of failure
Agent based Cloud IDS [31]	NIDS	Signature-based	Outside of cloud network	No implementation	Get the overall view of network traffic	Unable to detect new unknown attacks and inter-

						VM attack
EICIDS [32]	NIDS	Real Time	On each node	Custom Attacks	EICIDS may detects inter-VM attacks	Not fault tolerant since the architecture is centralised
Collaborative NIDS [33]	NIDS	Hybrid	On each cloud host and at the front end	Not provided	Can monitor both external and internal attack	Will result a complex configuration of a set of NIDS and the monitoring process will consume more resources
Collaborative IDS Framework for Cloud [34]	NIDS	Signature-based	On each cluster	KDDCup 99	Protect against DDoS attack	Requires more training samples

Table 3. Cloud IDS as a Service Research

Title	IDS Type	Detection Method	Positioning	Dataset	Advantages	Limitations
Cloud-based IDS [11]	NIDS	Signature-based	IDS as a service	Experiment are not being done	Reduce cost of managing IDS and cost of resource	Single point of failure and internal attack will be invisible.
SIDSCC [35]	NIDS	Signature-based	IDS as a service	ICMP Flood attack	Provide promising performance.	Did not detect unknown attacks
IDS as a service [36]	NIDS	Signature-based	Snort is provided as a web service	Custom dataset	Able to detect known attack.	Invisible to unknown or new attack.
CIDS [37]	Hybrid	Hybrid	IDS as a service	CIDD	Able to detect both known and unknown masquerade attack. Eliminate single point of failure.	The analysis may have delay because of the location of distributed analysis cloud.
A hierarchical, autonomous, and forecasting cloud IDS [38]	Hybrid	Hybrid	Located in a cloud node	CIDD	Detect more attacks than previous version	Single point of failure.
SaaSIDS [39]	NIDS	Hybrid	IDS as a service	Custom Dataset	Reduce cost of implementing IDS and human resource	The IDS can be flooded by the traffic of the client.
Rules based Enhancement in Cloud IDS Service [40]	NIDS	Signature-based	IDS as a service	Custom dataset	Able to eliminate single point of failure and increase availability of IDS service	Did not detect unknown attacks
Pub-Sub IDS [41]	NIDS	Signature-based	IDS as a Service	No Implementation	Prevent single point of failure	Unable to detect unknown attack

Table 4. Cloud IDS Research based on Open Source Approaches

Title	IDS Type	Detection Method	Positioning	Dataset	Advantages	Limitations
NIDS for Open Source Cloud [42]	NIDS	No explanation in the paper	On Virtual Machine Manager (VMM)	No explanation	The IDS has a good performance result based on the resource usage	No IDS performance result based on detection rate
IDPS [44]	NIDS	Hybrid and prevention	Traditional Network location	No explanation	Able to detect both known and unknown attack	Inter-VM attack will be invisible from IDS
Incorporating Honeypot for IDS in Cloud [43]	NIDS	Hybrid	Cluster Controller (Eucalyptus framework)	Custom dataset	Detect known and unknown attacks. Controlled use of honeypot generates less number of false alarms for unknown Attacks.	Need some improvement in detecting high level of security threat
Integrated IDPS with honeypot on cloud computing environment [45]	NIDS	Hybrid	Within Cloud Network	Own dataset	Detect and prevent internal attack	The honeypot is useless if no attack targeting them
SnortFlow [46]	NIDS	Signature-based	Domain 0	Custom dataset	Performance is good in handling multiple packets	Unable to detect inter-VM attacks
Snort for Cloud IDS [47]	NIDS	Signature-based	Behind gateway	No implementation	Provide overall perimeter protection for cloud	Unable to detect inter-VM or internal attack
Suricata and KVM Cloud IDS [48]	NIDS	Signature-based	On multiple places	No information	Reduce cost	Unable to detect unknown attacks
Integrated Open Source Cloud IDS [50]	Hybrid	Signature-based	Hypervisor	Not describe	Cost effective solutions	Redundancy of NIDS may sacrifice performance
IDS for private Cloud [51]	Hybrid	Hybrid	In VM host	KDD99	95.5% detection rate.	Can be expand with real implementations

Table 5. Cloud IDS Research in Machine Learning approaches

Title	IDS Type	Detection Method	Positioning	Dataset	Advantages	Limitations
Self-similarity IDS [64]	HIDS	Anomaly based	On each cloud host	DARPA 1999	May work robustly even though the Windows event log does not include enough information. Short learning periods.	Did not detect co-residency attack
Network activity classification	NIDS	Anomaly based	Behind Router	Not describe	Detecting unknown attack based on	Unable to detect inter-VM or internal attack.

and log audit for cloud computing [52]					traffic analysis	
Virtual HIDS for Cloud [53]	NIDS (even the title HIDS)	Anomaly based	Behind router	CIDD	Up to 80% TPR	Unable to detect inter-VM or internal attack.
Detecting DoS attack in cloud computing environment using covariance matrix [54]	NIDS	Anomaly-based	Domain 0	Custom attack	Able to detect the DoS	
HMM prediction model [55]	NIDS	Hybrid	On VMM	LLDDoS1.0	Successfully fired the early warning alerts before the launching of the attack	Require further testing with other attacks.
GA Cloud IDS [56]	NIDS	Signature based	On domain 0	No implementation	GA with fixed generational iteration helps in enhancing the security features	Did not detect unknown attack.
ANN Cloud IDS [59]	HIDS	Anomaly-based	VMM	No information	Increases resource availability and optimise IDS resource utilisation	Unable to detect network-based attack
HIDS for Cloud [60]	HIDS	Signature based	On each cloud host	Custom System Call dataset	Up to 96% of accuracy	Unable to detect novel attack and the system did not provide real time implementation.
Smith-Waterman GPU Cloud IDS [61]	HIDS	Signature-based	On Domain 0	Custom co-residency attack	Six times faster performance	Unable to detect unknown attack.
ANN Cloud IDS [62]	NIDS	Anomaly-based	On the switch.	ISOT dataset	Provide great accuracy result	Unable to detect internal attacks
GA Cloud IDS[57]	NIDS	Anomaly-based	Simulation	Custom dataset	57% detections of random sets of cloud attacks	The detection rate can be improved in the future works
FC-ANN Cloud IDS [63]	NIDS	Anomaly-based	On the switch	Not implemented	Improve the result of ANN Cloud IDS	Single point of failure when implemented IDS on switch.
Differential Game Model [66]	Numerical Analysis	Anomaly-based	MATLAB Simulation	No explanations	Improve cloud security and reduce energy consumption	Requires more explanation on the experiment in real environment.
DCA CloudIDS [68]	Hybrid	Hybrid	Virtual Switch and Each Cloud VM	DARPA 1999	Total protection for every part of Cloud IDS	Did not handle very well in term of high traffic data

Table 6. Summary of Cloud IDS Research

Title	**IDS Type**	**Co-residency detection**	**Data Privacy Concern**	**Real-time Detection**
Livewire [16]	HIDS	No	Yes	Yes
Intrusion Detection in the Cloud [18]	NIDS	No	Yes	Yes
Distributed intrusion detection in clouds using mobile agents [34]	Hybrid	No	No	Yes
Intrusion Detection for Grid and Cloud Computing [3]	Hybrid	No	No	No
Distributed Cloud IDS [26]	NIDS	No	No	No
NIDS for Open Source Cloud [42]	NIDS	No	No	Yes
SIDSCC [35]	NIDS	No	No	Yes
Self-similarity IDS [64]	HIDS	No	No	No
Cloud-based IDS [11]	NIDS	No	No	No
IDS as a service [36]	NIDS	No	No	Yes
CIDS [37]	Hybrid	No	No	Yes
IDPS [44]	NIDS	No	Yes	No
Collaborative intrusion detection [15]	Hybrid	Yes	No	Yes
Adaptive Distributed IDS for Cloud Computing [28]	NIDS	Yes	No	No
Incorporating Honeypot for IDS in Cloud [43]	NIDS	No	No	Yes
Fingerprinting system calls approach for IDS in Cloud [21]	HIDS	No	No	No
A hierarchical, autonomous, and forecasting cloud IDS [38]	Hybrid	No	No	Yes
Network activity classification schema in IDS and log audit for cloud computing [52]	NIDS	No	No	No
Virtual HIDS for Cloud [53]	NIDS	No	No	No
Integrated IDPS with honeypot on cloud computing environment [45]	NIDS	No	No	No
SnortFlow [46]	NIDS	No	No	Yes
Detecting DoS attack in cloud computing using covariance matrix [54]	NIDS	No	No	Yes
SaaSIDS [39]	NIDS	No	No	Yes
Rules based Enhancement in Cloud IDS Service [40]	NIDS	No	No	No
Mini-IDS [29]	NIDS	No	No	No
Pub-Sub IDS [41]	NIDS	No	No	No
IRAS [30]	NIDS	No	No	No
HIDS for Cloud [60]	HIDS	No	No	Yes
HMM prediction model [55]	NIDS	No	No	Yes
GA Cloud IDS [56]	NIDS	No	No	No
Snort for Cloud IDS [47]	NIDS	No	No	No
Agent based Cloud IDS [31]	NIDS	No	No	No
ANN Cloud IDS [59]	HIDS	Yes	No	No
EICIDS [32]	NIDS	Yes	No	Yes
Smith-Waterman GPU Cloud IDS [61]	HIDS	Yes	No	Yes
Suricata and KVM Cloud IDS [48]	NIDS	Yes	No	Yes
ANN Cloud IDS [62]	NIDS	No	Yes	No
Integrated Open Source Cloud IDS [50]	Hybrid	Yes	No	Yes
FC-ANN Cloud IDS [63]	NIDS	No	No	No
Collaborative NIDS [33]	NIDS	Yes	No	Yes
Collaborative IDS Framework for Cloud [34]	NIDS	Yes	Yes	No
GA Cloud IDS[57]	NIDS	No	No	No

IDS for private Cloud [51]	Hybrid	Yes	No	No
NvCloudIDS [22]	Hybrid	Yes	No	No
Differential Game Model [66]	Numerical Analysis	No	No	No
DCA CloudIDS [68]	Hybrid	Yes	Yes	Yes