CloudIDS: Cloud Intrusion Detection Model Inspired by Dendritic Cell Mechanism

Azuan Ahmad, Norbik Bashah Idris and Mohd Nazri Kama

Advanced Informatic School. University of Technology Malaysia, 54100 Kuala Lumpur, Malaysia

***Abstract*:** Cloud Computing Security is a new era of computer technology and opens a new research area and creates a lot of opportunity of exploration. One of the new implementation in Cloud is Intrusion Detection System (IDS).There are problems with existing IDS approach in Cloud environment. 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 consumes more time where not each Cloud user has. A decentralized traditional IDS approach where being deployed in current Cloud Computing infrastructure will make the IDS management become complicated. Each user's IDS will not be the same in term of type and configurations and each user may have outdated signatures. Inter VM's communication also become a big concern when we implementing Cloud Computing system where communication between Clouds are not monitored and controlled by the traditional IDS. A specific IDS model for Cloud computing is required to solve these problems. In this paper, we develop a prototype of Cloud IDS inspired by Dendritic Cell mechanism. Experiment result proved that Cloud IDS was able to detect any attempt to attack the Cloud environment. The experiments show that the Cloud IDS model based on Dendritic Cell algorithm able to identify and detect novel threat that targeting Cloud environment.

***Keywords*:** cloud computing, information security, artificial immune system, intrusion detection, dendritic cell, artificial immune system

1. Introduction

With the development of communication networks, Cloud Computing has become critical technology to a modern society. The explosive growth of Internet and Cloud users has motivated the rapid expansion of electronic commerce and other online-based services. Behind convenience and efficiency resulted from these services, there lies a dark side, vulnerability to cyber threats.

As our lifestyle that always depends on network technology or more specifically Internet, we are exposed to at least one of the attacks. In the recent year, even high profile Internet companies like Google, Apple, eBay and Yahoo were hacked by intruders [1]. In Malaysia, estimated losses from electronic hacking are reaching RM 3.3 million within 2012[2]. The increasing importance of computer security motivates various angles of security related research that provide new solutions, which might not be achievable by more conventional security approaches.

Cloud Computing is the new concept of computing where people only need to pay for services and resources without need to place any cost for pysical hardware. With the implementation of Cloud Computing in the application today, it emerges a new technique in software developmnet and deployment. It also change 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 [3].

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. When organizations and companies which are using Cloud Computing services, they will move their resource from their own 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 source [4]. 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.

In addition, there are no specific Intrusion Detection System (IDS) built to protect Cloud Computing systems. 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. This traditional IDS implementation, such as on virtual machines (VM), which is considered more vulnerable with diverse security requirements [5]. 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 consumes more time where not each Cloud user has [6, 7]. 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.

In addition, a decentralized traditional IDS approach where being implemented in current Cloud Computing infrastructure will make the IDS management become complicated. Each Cloud user will install their own IDS and the Cloud Provider will have no authority in managing each Cloud User's IDS. This approach also will affect the services that provided by each Cloud User if the IDS were installed on the host of the Cloud Provider. At the same time, if the

IDS was installed traditionally in the Cloud infrastructure and managed traditionally. Each user's IDS will not be the same in term of type and configurations and each user may have outdated signatures. If any attack happens, then each Cloud User's IDS will not treat the event the same way and some of the IDS may not even detect that event. This will bring risk not only to the Cloud User itself but also to the other Cloud Users and in worst case will also affect Cloud Provider and the whole system.

Inter VM's communication also become a big concern when we 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 occurs and at the same time to block the events from occurring.

2. Related Works

This research considered to be 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.

J. Arshad et al. proposed an intrusion severity analysis for cloud computing where in their research, they used the hybrid approach where the attack were detected based on the attack database that they provide and from the Profile Engine (PE) which 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 [8]. 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.

Normal implementation of cloud infrastructures includes the deployment of virtual machine monitors (VMM). Hence, this research also related to the research based on VMM. Garfinkel .T and Rosenblum .M proposed the virtual machine introspection based architecture for intrusion detection [9]. Virtual machine introspection (VMI) is the process of monitoring and inspecting a virtual machine from the outside for the purpose of analyzing the software running inside it [10]. 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.

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 [11]. 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 module; Data Logging Module, Preprocessing 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 are able to achieve the accuracy with a high sensitivity of 96%.

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 [12]. 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.

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 [13]. 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.

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 [14]. The author did not provides any experiments and results from this research.

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 [16]. 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.

In their paper [17] proposed a novel Collaborative IDS Framework for Cloud computing environment. 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 DDoS attacks and increase the performance and accuracy of IDS. However, it requires a high training time.

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 [15]. 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 analyzed for the identification of threats. Thus, the entire

Table 1 provides an analytical study on the related works

	IDS Type	**Detection Method**	**Positioning**	**Dataset**	**Advantages**	**Limitations**
Intrusion Severity Analysis [8]	HIDS	Hybrid	On Domain 0	Own generated dataset	Successfully demonstrate the effectiveness of the intrusion severity analysis method	Dataset and may be questionable
Livewire [9]	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 administrator responds to that event
HIDS for Cloud ([11])	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.
NIDS for Open Source Cloud [12]	NIDS	No explaination in the paper	On Virtual Machine Manager (VMM)	No explainati on	The IDS has a good performance result based on the resource usage	No IDS performance result based on detection rate
Self-similarity IDS [13]	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.	
Collaborative intrusion detection [14]	Hybrid	Real Time	On each node	No explainati on	May detects both Network attacks and host attacks.	Need more explanations about the experiments and analysis.
EICIDS [15]	NIDS	Real Time	On each node	Custom Attacks	EICIDS may detects inter-VM attacks	Not fault tolerant since the architecture is centralised
Collaborative NIDS [16]	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 [17]	NIDS	Real Time	On each cluster	KDDCup 99	Protect against DDoS attack	Requires more training samples

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. **Error! Reference source not found.** illustrates the architecture of EICIDS.

Table 1 provides an analytical study on the related works based on the Cloud environment protection by using IDS.

3. Dendritic Cell Mechanism

This section describes Dendritic Cell process and their components.

3.1 Dendritic Cell Inspiration

Dendritic cells (DC) are the main function in natural immune system by which the innate immune system collects and present antigens to the adaptive immune system for processing. Dendritic cell exist within three states immature, semi-mature and mature dendritic cell where immature dendritic cells are reside in tissues throughout the body for collecting antigens and signals for processing, semi-mature dendritic cells is the results from immature dendritic cells that collect antigen and signal in a environment that have safe signal more than danger signal and mature dendritic cell on the other hand is the results from immature dendritic cells that collect antigen and signal in a environment that have danger signals more than safe signals. Dendritic cells are especially abundant in tissues where pathogens may enter body, such as skin, lung and gastrointestinal tract. Figure 1 simulate the Dendritic Cell Maturation Process by stimulation of various signal

3.2 Antigen

Dendritic cells ingest nearby pathogens and cellular debris and process this ingested material and use molecular structures on their surfaces to present any antigen found. Dendritic cells also bind with signaling molecules that affect their functioning and provide stimulus for maturation.

As they mature, dendritic cells leave the peripheral tissues and migrate to the lymph nodes and other lymphatic organs. In the paracortex of lymph node, a dendritic cell interacts with lymphocytes, such as T-cells presenting antigens for further processing by the adaptive immune system.

3.3 Signals

The Danger Model holds that the maturation of dendritic cells is controlled by signaling molecules named Pathogen Associated Molecular Pattern (PAMP), danger, safe and inflammation signals found in the surrounding tissue. Tissues experiencing stress or damage emit danger signals while healthy, unstressed tissues emit safe signals. Some molecular patterns commonly found along with bacteria and other pathogens also act as danger signals.

Sufficient stimulus by danger signals causes dendritic cells to become fully mature. This causes them to express signaling molecules that indicate the antigens they present were found in a dangerous environment. Mature dendritic cells promote immune reactions to the antigens by the adaptive immune system. On the other hand, sufficient stimulus by safe signals causes the dendritic cells to become semi-mature. Semi - mature dendritic cells indicate that their antigens were collected in a safe environment and tend to suppress immune response to these antigens [18].

PAMPs are molecules produced my microorganism. These molecules are not unique to pathogens but are produced by microbes. PAMP molecules are an indicator to human immune system that a non-host entity was presented. Specific PAMPs bind to specific receptors on dendritic cells which can lead to production of both co-stimulatory molecules and interleukin-12 (IL-12) which related to danger signal. In our

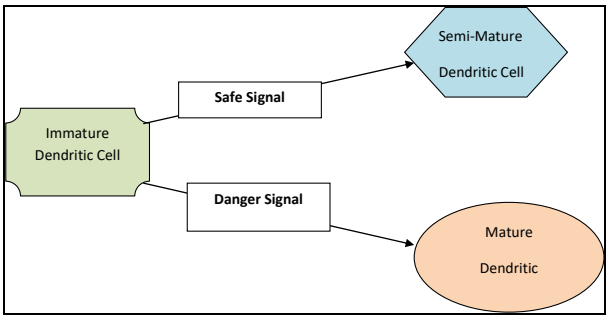

Figure 1. Dendritic Cell Maturation Process

immune system, PAMPs is as a biological signature of abnormality. In this Cloud IDS model, PAMP is interpreted as a signal which is an indicator of an abnormality. This is presented by the detection of intrusion based on detection signature.

Danger signals are the signals release when a necrosis happens in the tissue cells. Necrosis is the unexpected or forced death of tissue cell that indicate something abnormal was happened in the tissue. The release of danger signal is the indicator of damage to the tissue against which the immune system is trying to protect. The sufficient exposure to the danger signal causes DC maturation to the fully mature state. Potency of danger signal is less than PAPMs, meaning that a higher concentration of danger signal molecules are needed in order to produce a response of the same magnitude as similar concentration of PAMPs. Concentration is the number of molecules of signal per unit volume. Within this thesis, danger signals are indicators of abnormality but have lower value of confidence that the PAMP signal. Danger signals expression is an indication that antigen in a dangerous context thus lead to the activation of the adaptive immune system [19].

Safe Signals is the signals release as a result of healthy tissue cell functions normally released during a normal cell death or known as apoptosis in medical term. A molecule named Interleukin-10 (IL-10) is produced as a result of the presence of safe signal in the tissue. The production of IL-10 indicates that antigen collected by DC was found in a normal, healthy tissue thus will suppress the immune reaction to the antigen. When a tissue contains cells undergoing both apoptosis and necrosis, the receipt of safe signal will suppress the production of IL-12 molecules is response to the danger and PAMP signals present in the tissue. This is one of the mechanisms in the immune system to prevent false positives.

4. Algorithm

This section explains the algorithm of DC mechanism for Cloud IDS model. Inspired by the activity of DC in human

tissue, Cloud IDS model try to mimic the same process as a solution in protecting Cloud network from intrusions.

Depicted in Figure 3, each monitored Cloud network activity is viewed as Antigen and the Internet Protocol (IP) address of each packet is taken as the Antigen identity. The Cloud IDS perform multiple signal and antigen sampling. Cloud IDS model will collect three signals from the Cloud environment; PAMP, Safe Signal and Danger signals linked to a specific antigen that trigger that signals. The signals then will be cumulatively group based on the DC. In our experiment, we consider each DC handles a specific antigen. Based on the collected input signals, the DC will be transform into either three outputs states; co-stimulatory signal (CSM), semi-mature and mature. When the DC exceeds the maturation threshold, in our case the monitoring time limit, the DC stop monitoring and the output signal values will be analysed. When learning ends, antigens appear in different contexts. In the last step, the potential anomalous antigen is determined based on the collected context known as the mature context antigen value (MCAV), the anomalous antigen is determined as:

$$MCAV = \sum \text{mature} / (\sum \text{mature} + \sum \text{semi-mature}) \quad (1)$$

The antigens with a greater than the anomaly threshold are classified into the anomalous group while the opposite are considered as the normal category.

5. Cloud IDS Model

This section describes Cloud IDS model, a model for detecting any threat and intrusion attempt for Cloud environment. Cloud IDS model imitate the functionality of dendritic cells in human immune system that protect our body from infection of pathogen and bacteria. This work is an enhancement of the work of Al-Dhubani et al [20]. This work expands the capability of Dendritic Cell Mechanism in analysing real world problems regarding the attack detections in Cloud Computing environment.

The Cloud IDS Model draws inspiration from the dendritic cell maturation process of the natural immune system. Figure 2 depicts an overview of the Cloud IDS model. This model synthesizes antigens from packets observe on the cloud network. It also synthesizes danger model signals from observed events and the state of the network and guest cloud. This model then classifies antigens as dangerous or safe and provides this information in detecting any threat to the Cloud environment.

The Cloud IDS model emulates and make use of the functions and activity of the dendritic cells in the body tissue of the HIS and applying the concept in protecting Cloud

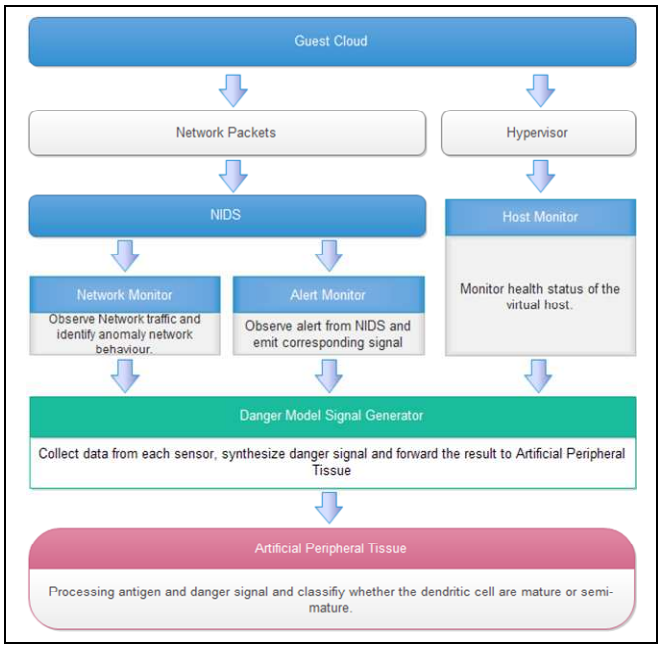

Figure 2. Cloud IDS model

environment. This model consists of a set of danger model signal generator, a misuse-based network intrusion detection system (NIDS) and artificial peripheral tissue (APT) where the dendritic cells, antigens and danger model signals interact.

Emulating the activity of dendritic cell required this model to have two most important elements of immune system, antigen and signals. Cloud IDS model captures and decomposes network packets collected from the private cloud environment and at the same time, antigens will be extracted from the network packets by the selected features of the network packets. This model also synthesizes danger model signals from external data sources.

This model provides two types of output, the sequence of alerts from the misuse-based NIDS and a sequence of artificial dendritic cells which presenting processed antigens and their corresponding dangerous or safe context. The dendritic cells then are process in the APT to get the maturation level of each cloud area. Figure 3 presents the elements of Cloud IDS model and the flow of data in this model.

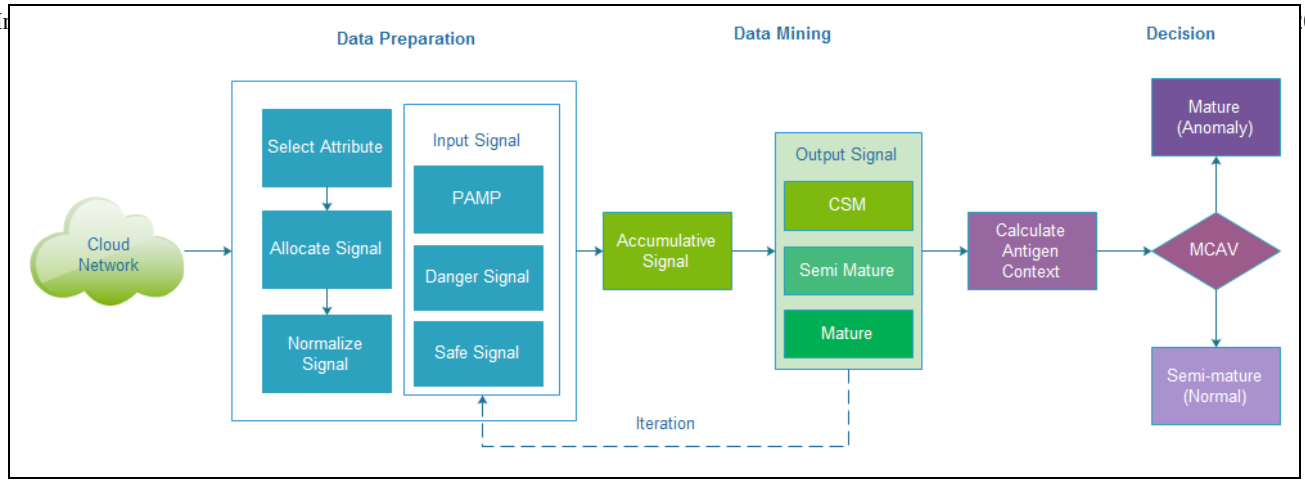

Figure 3. Algorithm for Cloud IDS model based on Dendritic Cell mechanism

5.1 Antigens and Signals Representation

Cloud IDS model uses two primary source of information as a primary data; antigens and signals. The antigen represents the cloud network traffic, which each monitored network packet resulting in the synthesis of a corresponding antigen.

Cloud IDS model contains two types of feature; address and protocol features. Address features are 32-bit, unsigned integer value Internet Protocol version 4 (IPv4) address found in the packet header information. Example of address features are 192.168.0.1 and 172.16.112.20. IPv4 address is used as the source or destination address for every network communications. On the other hand, protocol features are 32-bit, unsigned integer derived from the protocol value found in the IPv4 packet header information. There are two commonly used protocols available Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) and for each protocol, port number is assign to represent what service they provide. Port number is the least-significant 16-bits of the feature in the packet header information, bits 0 to 15.

Cloud IDS model collects signals from the Cloud network by implementing signal sensors on each Cloud node. Each Cloud node consists of three signal sensors; host monitor, alert monitor, and network monitor. Each signal includes two functional elements. The first element is the antigen feature value where this indicates the antigen that produces the signals. The second element is the signal level. This is an integer value that determines the degree of danger or safety each corresponding signal represents. A signal with high level of danger signals indicate a signal was collected in an area of danger and on the other hand, a signal with high level of safe signal indicate that the signal was collected in a safe area.

5.2 Host Monitor

Host monitor observe the state of each guest cloud host and emits signal based on the health status for each of the Cloud user. The state of the cloud host will affect the immune response in Cloud IDS similar as in HIS where the tissue states affect the response of the human immune system. Any host state that showing the damage on the host promotes immune reactions while healthy host state suppresses immune reaction.

Host monitor continuously monitor the status of each cloud host in the cloud environment by using multi-agent system. When activated, host monitor gather monitoring data using agent that installed on each Cloud host through secured channel. Figure 4 describe the Host Monitor activity in monitoring each Cloud nodes.

5.3 Network Monitor

Network Monitor observes and analyse network traffic in the cloud network and emitting danger signal based on the state of the network traffic. Network Monitor identify anomaly in the cloud network by comparing the current network behaviour with the normal traffic behavior or known as normal traffic profile. Network behavior that significantly different from the normal traffic profile are an indication of anomaly and result in emission of danger signals. Observations that similar or within the normal traffic profile is considered normal and result in emission of safe signals.

Network monitor assist Cloud IDS in detecting any anomalous cloud network traffic that may indicate a threat to the cloud environment by emitting or suppressing related signals. This process is analogous to the effect of tissue stress on the HIS. Tissue under stress emits chemical signals that promote immune response while unstressed tissue suppresses immune reactions.

5.4 Alert Monitor

Alert monitor analyse the alerts emitted by the NIDS and generate a corresponding danger signal. This will results evidence of danger seen in the network packets to affect the immune response. This is inspired by the ability of dendritic cells in detecting the presence of pathogens through reaction to Pathogen Associated Molecular Pattern (PAMP) signals collected in body tissue.

6. Experiment

Testing the performance of Cloud IDS model is crucial in measuring the ability the Cloud IDS in detecting intrusion targeting the Cloud environment. This section explained the experiment conducted in measuring the ability of Cloud IDS in detecting intrusions from DARPA 1999 dataset. Figure 4 describe the design of the experimental Cloud network.

There are five weeks of collected data forming by the normal and attacks data recorded within DARPA 1999 dataset. It consists of 201 instances of about 56 types of attacks distributed throughout the testing data which is included in the fourth and fifth weeks of the dataset [21]. This research

only focused on the testing data (Week 4 and Week 5) and both weeks of data were running through the cloud networks using *Tcpreplay* and the response were recorded and analysed.

The DARPA 1999 data consist of separate data sets for each day of evaluation. A single day of evaluation run for 22 hours of operational time and each of these days represents a stand-alone intrusion detection scenario. Each day Cloud IDS will run an independent experiment with initial state. The output data for each day is the form of a set of collected signals with antigens. Both of antigen and their signals was cumulatively calculated and produce the Mature Context Antigen Value (MCAV) for each day. The MCAV for each antigen describes the anomaly value of each antigen. If the MCAV of the antigen exceeds the MCAV threshold, the antigen is classified as anomalous and vice versa.

DCA is directly based on the correct mapping of signals. For the evaluation of Cloud IDS performance with DARPA 1999 dataset, eleven signals were derived from behavioural attribute of the monitored victim cloud host: one PAMP, six danger signals and four safe signals. Sensing intrusion from more signals will bring more accurate detections to the Cloud IDS model. The PAMP signals is collected from data source which obviously indicate an attack. Danger signals (DS-1, DS-2, DS-3 and DS-4) are taken from attributes which represent changes in behaviour. Safe signals (SS-1, SS-2, SS-3 and SS-4) are also taken from changes in behaviour but high safe signal values are collected from a normal behaviour condition. In selecting appropriate signals and other attributes such as average and standard deviation of each data, a number of preliminary experiments must be performed. The signals used in this experiment are network-based attributes and this data is the most variable data under attack conditions. Each signal are categorised into different module of Cloud IDS model; PAMP under Alert Monitor Module, DS-1, DS-2, DS-3, DS-4, SS-1, and SS-2 under Network Monitor module and DS-5, DS-6, SS-3 and SS-4 under Host Monitor module. Table 2 summarizes classification of signals for Cloud IDS sensor module.

Table 2. Cloud IDS module and signals classification

Cloud IDS Module	Signal	Sensor
Alert Monitor	PAMP	Alert Sensor
Network Monitor	SS-1, SS-2, DS-1, DS-2, DS-3, DS-4	Inbound Network Traffic sensor, Outbound Network Traffic sensor, SYN Packet Rate sensor, ICMP Unreachable Packet Rate sensor
Host Monitor	SS-3, SS-4, DS-5, DS-6	Memory Usage sensor, CPU usage

7. Result and Discussion

The result is the comparison between the detected anomalous activity output and the DARPA IDEVAL 1999 Master Identification List. The same criteria that determine results for True Positive, False Negative and False Positive detections in the misuse-based NIDS baseline performance also apply to results for the Cloud IDS performance. Table 3 shows the CloudIDS detection results based on DARPA 1999 master identification list.

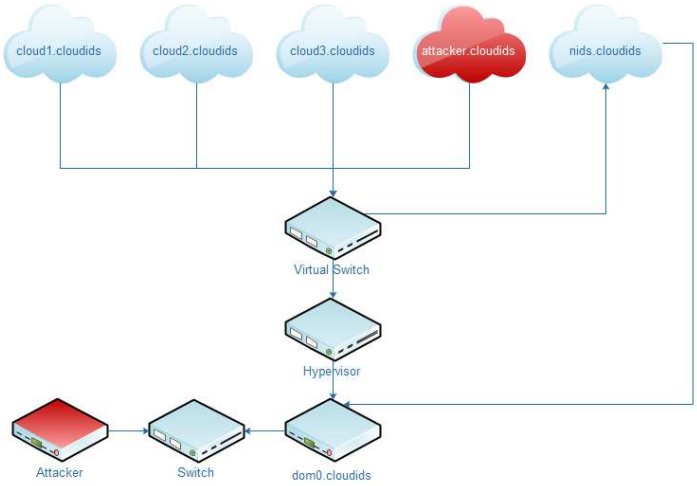

Figure 4. Cloud IDS model experimental network used for experiment

Table 3. CloudIDS Performance Result

DARPA 99 WEEK / DAY	Number of Threats Events (P)	True Positives Detections (TP)	False Positives Detections (FP)	False Negative Detections (FN)
W4D1	17	8	0	9
W4D2	N/A	N/A	N/A	N/A
W4D3	19	14	6	5
W4D4	15	12	7	3
W4D5	17	12	1	5
W5D1	26	20	2	6
W5D2	24	10	1	14
W5D3	16	11	5	5
W5D4	21	6	0	15
W5D5	32	19	7	13
TOTAL	**187**	**112**	**29**	**75**

Figure 5 and Figure 6 shows the result of the True Positive value and Positive Predictive value comparison between CloudIDS, baseline performance result and NetTRIAAD respectively [22]. From the table, there is a significant statistical improvement that CloudIDS perform based on the True Positive Rate and Positive Predictive Value. The result can be improved based on the selection of the signals because more signals may produce more accurate results. From the comparison, CloudIDS improves sensitivity in detecting intrusions compared to baseline performance and NetTRIAAD model at the same time provides an improved accuracy results.

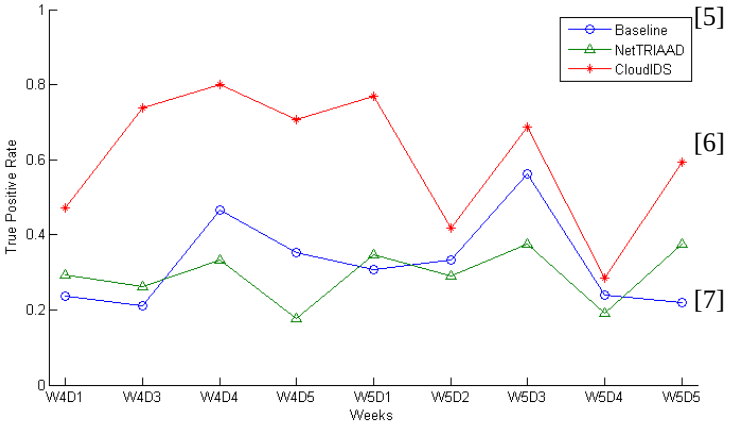

Figure 5. True Positive Result comparison with NetTRIAAD

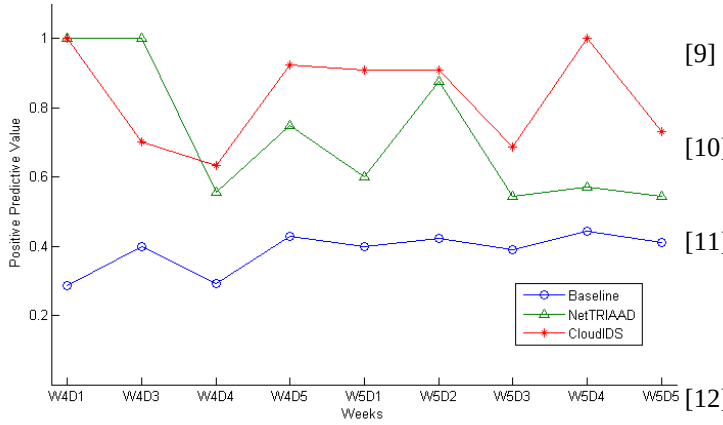

Figure 6. Positive Predictive Value comparison with NetTRIAAD

8. Conclusion

In this paper, IDS methodology was combined with Dendritic Cell Algorithm mechanism to provide a solution in detecting any attack targeting the Cloud environment. Cloud IDS model mimics the activity and process of Dendritic Cell which is known for detecting and killing any pathogens that infected human tissue and cells. The successful of Dendritic Cell in protecting human body will also bring a success in protecting Cloud environment if the same mechanisms are being implemented in the real world applications.

References

[1] BBC, "Google and Apple among hundreds hit in high-profile Pakistan hack," 26th November, 2012 2012.

[2] CyberSecurity. (2012, 19th November 2012). *Hacking costs Malaysia MYR 3.3 million*. Available: http://www.cybersecurity.my/en/knowledge_bank/news/2012/main/detail/2249/index.html

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

[4] D. Gollmann, "Computer security," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 2, pp. 544-554, 2010.

[5] 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.

[6] I. Cymtec Systems. (2012). *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

[7] 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*, 2012, pp. 213-218.

[8] 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.

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

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

[11] 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.

[12] 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*, 2010, pp. 265-270.

[13] 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*, 2011, pp. 353-362.

[14] 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*, 2012, pp. 91-109.

[15] 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.

[16] 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.

[17] 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.

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

[19] P. J. Bentley, J. Greensmith, and S. Ujjin, "Two ways to grow tissue for artificial immune systems," in *Artificial Immune Systems*, ed: Springer, 2005, pp. 139-152.

[20] N. B. I. Raed Al-Dhubhani, Faisal Saeed, "A Prototype for Network Intrusion Detection System using Danger Theory," *Jurnal Teknologi*, vol. 73, p. 8, 12 February 2015 2015.

[21] D. Dasgupta and H. Brian, "Mobile security agents for network traffic analysis," in *DARPA Information Survivability Conference & Exposition II, 2001. DISCEX'01. Proceedings*, 2001, pp. 332-340.

[22] R. L. Fanelli, "Further experimentation with hybrid immune inspired network intrusion detection," in *International Conference on Artificial Immune Systems*, 2010, pp. 264-275.