Cloud Intrusion Detection Model Inspired by Dendritic Cell Mechanism

Azuan Ahmad
Advanced Informatic School
University of Technology Malaysia
54100 Kuala Lumpur, Malaysia
azuan2@live.utm.my

Nor bik Bashah Idris
Advanced Informatic School
University of Technology Malaysia
54100 Kuala Lumpur, Malaysia
nor bik@utm.my

Mohd Nazri Kama
Advanced Informatic School
University of Technology Malaysia
54100 Kuala Lumpur, Malaysia
mdnazri@utm.my

Abstract—Cloud Computing Security is a new implementation 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 the implementation of 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 implemented 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 Each user’s IDS will not be the same in term of type and configurations and each user may have outdated signatures.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 implementation. 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.

Keywords—cloud computing; information security; artificial immune system; intrusion detection; dendritic cell

I. 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 physical hardware. With the implementation of Cloud Computing in the application today, it emerges a new technique in software development 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
won’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.

II. RELATED WORKS

This section reviews the previous work related to Cloud IDS research and prototypes. The number of research focusing in Cloud IDS is increasing rapidly and there are several solutions that researchers proposed to solve the issues in Cloud Security.

Tupaluka et al. proposed a model based on Virtual Machine Monitor (VMM) or we called Hypervisor within this paper to protect Cloud environment from various attack. This model works on Infrastructure layer of Cloud implementation. VMM have the control over the Cloud resource and this is an efficient way to detect intrusion on the Cloud environment because it has a good visibility of the Cloud resources including network and processing resource of every Cloud host [8].

Gustavo & Miguel in their paper provides a solution to protect Cloud in Software as a Service (SaaS) layer. In their paper, they found that anomaly IDS is a promising technique to be used to protect Cloud application layer [9].

Viera et al. proposed a Grid and Cloud Computing Intrusion Detection System (GCCIDS). Their prototype used Artificial Neural Network (ANN) as the machine learning algorithm to train the system and developing their prototype using Grid-M middleware. They proved that their system had low processing cost while maintaining satisfactory performance for real-time implementation, since it performed the analysis individually on each node, resulting in lower data exchanges between nodes, thus decreasing the complexity of the system [10].

III. DENDRITIC CELL MECHANISM

This section describes Dendritic Cell process and their components.

A. 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

B. 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 signalling 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.

C. Signals

The Danger Model holds that the maturation of dendritic cells is controlled by signalling 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 signalling 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.

PAMPs are molecules produced by microorganisms. 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 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.

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.

The presence of inflammatory signals in human tissue is insufficient to initiate maturation of an immature DC. However, the presence of inflammation not only implies the presence of inflammatory cytokines but also the temperature increased in the affected tissue. The rates of reaction also increased because of the increasing heat and inflammatory cytokines initiate the process of dilating blood vessels result in increased number of cells to the tissue under distress. In this model, inflammation has the effect of amplifying the other three categories of input signals. The result is an increase in the artificial DC's output signals.

Within Cloud IDS model, input signals that indicate normal activity are known as safe signal. This signal is interpreted as data which indicates normal system or data behaviour and high level of this signal will increase the output signal value for the semi-mature DC. The receipt of a high safe signal will reduce the cumulative value of the mature DC.

### IV. ALGORITHM

This section explains the algorithm of DC mechanism for Cloud IDS model. Inspired by the activities 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 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

![Cloud IDS model](image-url)
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 transformed into either three output 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 stops 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:

\[ \text{MCAV} = \frac{\sum \text{mature}}{\sum \text{mature} + \sum \text{semi-mature}} \]  

(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.

V. 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.

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 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.

A. 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

![Fig. 3. Algorithm for Cloud IDS model based on Dendritic Cell mechanism](image-url)
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.

B. 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 4.1 describe the Host Monitor activity in monitoring each Cloud nodes.

C. 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 behaviour or known as normal traffic profile. Network behaviour 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.

D. 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.

VI. 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 mechanism are being implemented in the real world applications.

References