Danger Theory Based Hybrid Intrusion Detection Systems for Cloud Computing

Azuan Ahmad, Bharanidharan Shanmugam, Norbik Bashah Idris, Ganthan Nayarana Samy, and Sameer Hasan AlBakri

Abstract—**Cloud Computing Security 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).There are problems with the implementation of existing IDS approach in normal environment.Traditional IDS need a lot of self maintenance and did not scale with the customer security requirements. The cost of maintaining and installing the traditional IDS is also a big consideration in implementing IDS in an organization. One of the solution of the problems in traditional IDS is by implementing it in Cloud environment. In Cloud, IDS can be managed centrally and can reduce the maintenance need to be done by a single company that use the IDS. The future IDS should come with reasonable cost, and reduced complexity with strong defensive mechanism. Thus, we propose an intrusion detection based on Software as a Service called Software as a Service Intrusion Detection Services (SaaSIDS) that not only for commercial solution, but also for open research communities. In this research, we focus on doing research on Software As A Service IDS (SaaSIDS) where traffic at different points of the network is sniffed and the interested packets would be transferred to the SaaSIDS for further inspection. The main engine of SaaSIDS is the hybrid analysis engine where the signature based engine and anomaly based engine which using Artificial Immune System (AIS) will work in parallel. The SaaSIDS is able to identify malicious activity and would generate appropriate alerts and notification accordingly.**

Index Terms—**Cloud computing, intrusion detection system, artificial immune system.**

I. Introduction

In recent years, the evolving of Intrusion Detection System (IDS) was increasing very fast and become a research trend for about twenty-five years [1]. Today, technology in IDS still expands and still used for their main functions to monitors, detects and responding to unauthorized activities and intrusions [2]. This paper will discuss on IDS and one of the detection technology that being implemented in IDS called Artificial Immune System (AIS).

A. Types of IDS

There are two types of IDS and being distinguished by their main functions: host-based IDS (HIDS) and network-based IDS (NIDS). HIDS is a type of IDS that monitors any changes to any single system and detects the illegal changes. They typically monitor logs, system calls, system activities etc in a way to detect any intrusion attempt to a system. HIDS are placed on a single host and requires a lot of installation if being implement in a large scale. HIDS on the other hand monitors inbound and outbound network traffic and detect if there are any intrusions. NIDS can be placed anywhere in the network and usually attached to any network devices or being installing independently [1].

HIDS only monitors the host that they are being installed and intrusion cannot be detected on other host. NIDS on the other side are placed on network and it monitors everything so it can detect any intrusion at the first place. The problem with NIDS is it cannot detect any packet that being encrypted or obfuscated.

B. Detection Approaches

IDS can be classified into two detection approaches: misuse detection and anomaly detection [3]. Misuse detection approach monitors network traffic or system activities for known misuse, most of the case using table of pattern called signatures. IDS will match the event with the signature to detect the event as misuse or not. Anomaly detection approach on the other hand, detects any intrusion based on its decision using some techniques including statistical and machine learning. The IDS will first learn about the normal behavior of the network or system and create a profile of it. If the is any event that did not match the profile is considered anomalous. Many researches have been done in this approach including neural network [4], statistical method [5] and [6].

Both detection approaches have their own pro and cons. Misuse detection are well known for its minimal false positives and for this reason a lot of commercial IDS implement this approach. The problem with this approach is it cannot detect any novel attack or intrusion due to outdated signature and cannot detect any attack that being obfuscated or encrypted. This problem can lead to false negatives. Anomaly detection approach is one of the solutions to detect novel intrusion but still have a lot of false positives. This becomes a bigger challenge when pattern of computer usage keep on changing over time. That brings a requirement for a dynamic profile of normal behavior [7].

C. Problems with Existing Intrusion Detection System

There are problems with the implementation of existing IDS approach in normal environment.

Traditional IDS need a lot of self maintenance and did not

Manuscript received April 18, 2013; revised June 21, 2013. This work was supported in part by Research Management Centre (RMC), Universiti Teknologi Malaysia through vote number R.K130000.7738.4D066.

The authors are with the Advanced Informatics School, Universiti Teknologi Malaysia Kuala Lumpur, Level 5, Razak Tower, Jalan Semarak 54100 Kuala Lumpur, Malaysia (e-mail: e-mail: azuan2@live.utm.my, bharani, norbik, ganthan, sameeralbakri @ic.utm.my).

DOI: 10.7763/IJCCE.2013.V2.267

scale with the customer security requirements. In addition, maintenance of traditional IDS requires expertise and consume more time that normal company did not have[8, 9]. 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 [9].

In order 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 [10]. 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 [8].

II. Cloud Computing

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 [11]. Cloud computing is based on five attributes: multi-tenancy (shared resources), massive scalability, elasticity, pay as you go and self-provisioning of resources.

There are three fundamental service model that are being implemented by cloud service provider [12]: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

A. Infrastructure as a Service (IaaS)

In the most basic cloud service model, providers of IaaS offer computers in physical or virtual machines and other resources. IaaS clouds often offer additional resources such as images in a virtual-machine image-library, raw and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles [13]. IaaS cloud providers supply these resources on-demand from their large pools installed in data centers. For wide-area connectivity, customers can use either the Internet or carrier clouds which are dedicated virtual private networks.

B. Platform as a Service

In the PaaS model, cloud providers deliver a computing platform typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. With some PaaS offers, the underlying computer and storage resources scale automatically to match application demand such that cloud user does not have to allocate resources manually.

C. Software as a Service

In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. The cloud users do not manage the cloud infrastructure and platform on which the application is running. This eliminates the need to install and run the application on the cloud user's own computers simplifying maintenance and support. What makes a cloud application different from other applications is its scalability. This can be achieved by cloning tasks onto multiple virtual machines at run-time to meet the changing work demand. Load balancers distribute the work over the set of virtual machines. This process is transparent to the cloud user who sees only a single access point. To accommodate a large number of cloud users, cloud applications can be multitenant, that is, any machine serves more than one cloud user organization. It is common to refer to special types of cloud based application software with a similar naming convention: desktop as a service, business process as a service, test environment as a service, communication as a service.

III. Human Immune System and Artificial Immune System

In IDS, one of the challenges is to differentiate between normal and harmful activities and some researchers study the behavior of Human Immune System (HIS) on how they protect our body from invaders.

HIS have two mechanisms called innate and adaptive response. Innate response will attract lymphocytes (a type of white blood cell in the human immune system) to the area of our body that injured and automatically consume dead cells. Different type of injuries have different types of innate response for example, if our body being hit by hard object, our body will response with swelling at the area of hit. The other HIS mechanism is adaptive response. It was a response the being learns during our lifetime such as antibody for certain disease. If a human being infected by a disease, T-cell and B-cell will digest the antigen (cell that bring the disease) and produce antibody to counter the disease and provide lifetime protection for that disease [7].

We can see the similarities between IDS detection approach and HIS response mechanism by referring to their function and behavior. Innate response is similar with misuse detection approach because both have specific detection signature and response. On the other hand, adaptive response has similarities with anomaly detection approach because both can differentiate normal and harmful activity or cells by learning the behavior of the body or network as shown it Table I.

TABLE I: RELATIONSHIP OF HIS AND IDS

HIS	IDS
Innate Response	Misuse Detection
Adaptive Response	Anomaly Detection

Since 1993 [7], researcher start to implement HIS to the IDS detection mechanism since HIS can be considered as an anomaly detection with minimal false negative and positive. Kephart et al [14], Forrest et al [15] and Somayaji et al [16] was among the first that introduce Artificial Immune System (AIS), computational intelligent inspired by HIS in IDS and this idea are still expanding among researchers. Kim et al [7] classified AIS implementation to IDS into three major roots:

1) Conventional Algorithms (example, IBM's Virus Detector) [14]
2) Negative Selection [15] and [16]
3) Danger Theory [17].

A. Conventional Algorithms

Conventional algorithm introduced by Kephart et al [14] was among the earliest attempt to apply HIS in IDS. Their research was more on automatic detection of computer viruses and worms because computer interconnectivity becoming more complex and traditional virus detection method (signature-based detection) will become less effective. Their aim was to create a virus detection system that detect and responds to virus or worms automatically.

They proposed a system using either of the fuzzy matching algorithms from a signature of viruses or using integrity monitors that monitor important binaries and data in the host for any changes. What makes their system unique is, to reduce false positive, if a binary was suspected as a virus, a decoy (a binary that created for being infected) will be exposed to the suspect and if the decoy are being infected, then they can confirm that that was a virus.

The problem with this paper is that, no details testing were given in their paper and they did not describe the algorithm in their paper since it was confidential.

B. Negative Selection

One of the three major roots of AIS was negative selection (NS). This technique implements the negative selection in the T-cell maturation process [15]. In negative selection, the process is eliminating any immature T-cells that bind to self antigens. This will make HIS to detect non-self antigens without mistake. So, any antigens with T-cells will automatically detect as non-self.

As proposed by Forrest et al [15], there are three phases of negative selection: defining self, generating detectors and monitor the anomalies. When defining self phase, it is the same process in normal anomaly detection where the system identified the normal behavior patterns. The next phase is generating detector where it generates a number of random patterns that will be compared to each self-pattern defined in the first phase. If any randomly generated pattern matches a self-pattern, this pattern fails to become a detector and thus it is removed. Otherwise, it becomes a detector pattern and monitors subsequent profiled patterns of the monitored system. In the last phase, the detector pattern will be match with any newly profile pattern and if the pattern did not match, then it was detected as anomaly.

C. Danger Theory

In danger theory, immune response is triggered by unusual death of self-cells. Burgess [18] proposed that an autonomous and distributed feedback and healing mechanism, triggered when a small amount of damage could be detected at an initial attack.

IV. RELATED WORKS

A. LYSIS

Hofmeyr [19] develop AIS for network intrusion detection called LYSIS. It has the NS detector algorithm for binary detector generation and implements various features of HIS such as activation, threshold, life span, memory detectors, costimulation, tolerisation period and a decay rate in order to monitor self and non-self behaviours. LYSIS will monitor network traffic and normal connections will be classified as self and the other will be non-self.

LYSIS was tested to 50 computers in a local area network (LAN) where each host area generating detectors and monitor new traffics with seven intrusions. The problem this research is they are using limited input data. It should be tested with more intrusions in the future works.

B. Danger Signal on Mobile Ad-hoc Network

Sarafijanovic and Le Boudec [20] implements Danger Signal (DS) on mobile ad-hoc network. Their method is classified packet loss as DS. They use the DS to prevent antigens entering NS process. When Protocols of events are collected at the nodes belonging to the route where the packet loss is observed and during the time close to the packet loss time, they are considered as non-self antigens. These non-self antigens are not passed to the detector generation process of the NS algorithm. Moreover, danger signals are used as co-stimulation signals confirming successful detection through a detector, with good performing detectors becoming memory detectors.

Their experiments were carried out on the Glomosim network simulator [21], where 5–20 nodes misbehaved among a total of 40 nodes. The final test results were:

1) The use of danger signals strongly impacted on the reduction of false positive error rates.
2) The addition of memory detectors also improved detection rates.

Once again, their system has the potential to be disposable, distributed, self-organised and light-weight, but has not been demonstrated in a realistic ad-hoc network yet.

V. Cloud Computing Intrusion Detection System

In our research, we are proposing on creating a novel cloud-based intrusion detection system inspired by artificial immune system especially on self non-self discrimination technique. This research will involve the development of private cloud-based IDS and being tested using real network traffic. We will also implement packet compression for improving data transfer between IDS agents and provide confidentiality to the data. The system will be tested by creating a cloud environment and monitor the network traffic for intrusions.

Traffic at different points of the network is sniffed and the interested packets would be transferred to the SaaSIDS for further inspection. The main engine of SaaSIDS is the hybrid analysis engine where the signature based engine and anomaly based engine which using artificial immune system will work in parallel as describe in Figure 1. The SaaSIDS is able to identify malicious activity and would generate appropriate alerts and notification accordingly. We believe the proposed approach offers new opportunities, providing economic, scalable and viable option to any Cloud-based users and satisfy the users' security demands.

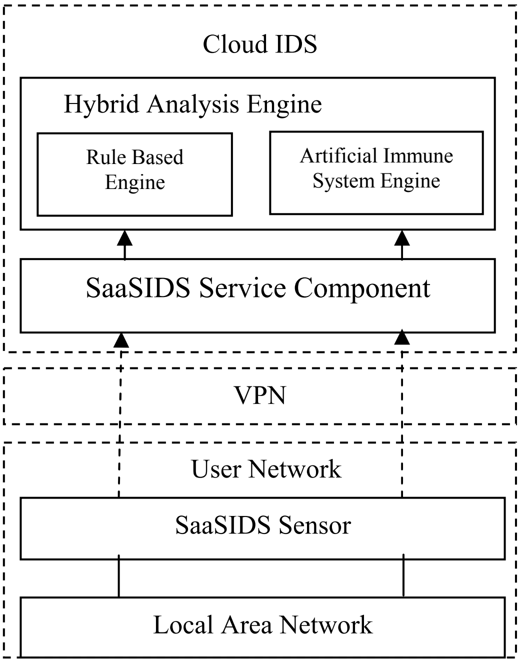

Fig. 1. SaaSIDS Architecture.

As described in figure 1, SaaSIDS consist of SaaSIDS sensor, SaaSIDS Service Component and Hybrid Analysis Engine that will be discussed in the following section.

A. SaaSIDS Sensor

SaaSIDS sensor is a device that installed on user's network to collect the selected packet before sending it towards Cloud IDS. SaaSIDS sensor also responsible for compressing and encrypting the packets to reduce the overhead during sending multiple packets into the Cloud IDS.

This device will be running on client side which it will monitor all the traffic flowing from and into the client and sending suspected packet to the SaaSIDS Service Component for further analysis.

B. SaaSIDS Service Component

SaaSIDS sensor is a device that installed on user's network to collect the selected packet before sending it towards Cloud IDS. SaaSIDS sensor also responsible for compressing and encrypting the packets to reduce the overhead during sending multiple packets into the Cloud IDS.

This device will be running on client side which it will monitor all the traffic flowing from and into the client and sending suspected packet to the SaaSIDS Service Component for further analysis.

C. Hybrid Analysis Engine

Hybrid Analysis Engine is the core component of the SaaSIDS. This component consists of two methods of analysis which are Rule Based Engine and Artificial Immune System Engine. Rule Based Engine will analyze the information received for intrusion detection based on the signature and if the information is not detected, Artificial Immune System Engine will analyze the packet by using anomaly based detection.

When the packet was received by SaaSIDS Service Component, Hybrid Analysis Engine will start to analyze the packet based on the Artificial Immune System (AIS) engine and Rule Based Engine as stated before.

VI. Conclusion

Since anomaly detection mechanism brings many false positive rates, it became a challenge to researchers and the research on this technique still going on. HIS from our body have minimal false negative rates and become inspirations for researcher for implementing it as AIS for IDS. Research in AIS open a new opportunity in IDS research and still a lot of rooms to grow and to be explored especially in cloud environment.

Acknowledgments

The authors would like to thank the Research Management Centre (RMC), Universiti Teknologi Malaysia for sponsoring this research through vote number R.K130000.7738.4D066.

References

[1] M. Tanase. (2001). The Future of IDS. [Online]. Available: http://www.securityfocus.com/infocus/1520

[2] O. M. P. Innella. (2001). An Introduction to Intrusion Detection Systems. [Online]. Available: http://www.securityfocus.com/infocus/1520

[3] R. Bace and P. Mell, "NIST special publication on intrusion detection systems," DTIC, Document, 2001.

[4] H. Debar, M. Becker, and D. Siboni, "A neural network component for an intrusion detection system," in *Proc. IEEE Computer Society Symposium*, 1992, pp. 240-250.

[5] H. S. Javitz, A. Valdes, and C. NRaD, "The NIDES statistical component: Description and justification," *Contract*, vol. 39, pp. 0015, 1993.

[6] S. S. Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, *et al.*, "GrIDS-a graph based intrusion detection system for large networks," in *Proc. The 19th National Information Systems Security conf.*, 1996, pp. 361-370.

[7] J. Kim, P. J. Bentley, U. Aickelin, J. Greensmith, G. Tedesco, and J. Twycross, "Immune system approaches to intrusion detection - A review," *Natural Computing*, 2007.

[8] I. C. Systems. (2012). Scout Cloud-Enabled IDS Fact Sheet. [Online]. Available: http://go.pardot.com/l/12332/2012-04-16/kjv2/12332/9341/Cymtec_Scout_IDS_Fact_Sheet_021412v2.pdf

[9] W. Yassin, N. Udzir, Z. Muda, A. Abdullah, and M. Abdullah, "A Cloud-Based intrusion detection service framework," in *Proc. 2012 International Conf.*, 2012, pp. 213-218.

[10] 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.

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

[12] W. Voorsluys, J. Broberg, and R. Buyya, "Introduction to cloud computing," *Cloud Computing: Principles and Paradigms*, Wiley Press, New York, 2011, pp. 3-41.

[13] H. S. A. Amies, Q. G. Tong, and G. N. Liu, *Infrastructure as a* Service *Cloud Concepts*, IBM Press, 2012.

[14] J. Kephart, G. Sorkin, M. Swimmer, and S. White, *Blueprint for a Computer Immune System*, Springer, 1999.

[15] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri, "Self-nonself discrimination in a computer," in *Proc. 1994 IEEE Computer Society Symposium*, 1994, pp. 202-212.

[16] A. B. Somayaji, "Operating system stability and security through process homeostasis," The University of New Mexico, 2002.

[17] P. Matzinger, "Tolerance, danger, and the extended family," *Annual review of immunology*, vol. 12, pp. 991-1045, 1994.

[18] M. Burgess, "Computer immunology," in *Proc. LISA-XII*, 1998.

[19] S. A. Hofmeyr and S. Forrest, "An immunological model of distributed detection and its application to computer security," The University of New Mexico, 1999.

[20] S. Sarafijanović and J.-Y. Le Boudec, "An artificial immune system for misbehavior detection in mobile ad-hoc networks with virtual thymus, clustering, danger signal, and memory detectors," *Artificial Immune Systems*, Springer, 2004, pp. 342-356.

[21] X. Zeng, R. Bagrodia, and M. Gerla, "GloMoSim: A library for parallel simulation of large-scale wireless networks," in *Proc. Twelfth Workshop*, 1998, pp. 154-161.

Azuan Bin Ahmad is currently a PhD student in UTM KL.Previously he have bsc. hons. computer science (Information Security Assurance) in USIM, Malaysia and Msc computer science (Information Security), UTM, Malaysia. His research work is on cloud security and malware research. His current research is on Cloud-based Intrusion Detection System.

Bharanidharan Shanmugam has received his Ph.D from Univesriti Teknologi Malaysia and is attached to Information Assurance and Security Research Group, Advanced Informatics School, Universiti Teknologi Malaysia. His research interest is towards Network Security, Cloud computing, Intrusion detection systems and risk assessment. He has published works related to those areas. He is a member of IEEE and actively participates in the review process for many ɔurnals and conferences.

Norbik Bashah is a professor at ADVANCED Informatics School, Universiti Teknologi Malaysia and is attached to Information Assurance and Security Research Group. Hi sresearch interest is towards Network Security, Intrusion Detection systems, Soft computing etc. He is a Senior Member of IEEE and actively participates in Information Security research

Ganthan Narayana Samy is a senior lecturer in information security at the Informatics Department, Advanced Informatics School (UTM AIS), Universiti Teknologi Malaysia (UTM), Malaysia. He received her PhD in Computer Science from Universiti Teknologi Malaysia (UTM), Malaysia. His research interests include information security risk management, healthcare information systems security and information security policy

Sameer Hasan Albakri is a PhD student in information security at UTM), Malaysia. He obtained his Master in Computer Science (Data Communication and computer networking) from University of Malaya (UM), Malaysia. His research interests include information security, cryptography, mobile phone security, information security risk assessment and cloud computing security. For more information about the researcher, please refer to http://scholar.google.com.my/citations?user=swbyAHUAAAAJ&hl=en