A Cloud-Based Intrusion Detection Service Framework

W. Yassin[1], N.I. Udzir[2], Z. Muda[3], A. Abdullah[4] and M.T. Abdullah[5]
Faculty of Computer Science and Information Technology,
Universiti Putra Malaysia,
43400 UPM Serdang, Selangor Darul Ehsan, Malaysia
izura@fsktm.upm.edu.my

Abstract-- Intrusion Detection System (IDS) have become increasingly popular over the past years as an important network security technology to detect cyber attacks in a wide variety of network communication. IDS monitors' network or host system activities by collecting network information, and analyze this information for malicious activities. Cloud computing, with the concept of Software as a Service (SaaS) presents an exciting benefit when it enables providers to rent their services to users in perform complex tasks over the Internet. In addition, Cloud based services reduce a cost in investing new infrastructure, training new personnel, or licensing new software. In this paper, we introduce a novel framework based on Cloud computing called Cloud-based Intrusion Detection Service (CBIDS). This model enables the identification of malicious activities from different points of network and overcome the deficiency of classical intrusion detection. CBIDS can be implemented to detect variety of attacks in private and public Clouds.

Keywords-Intrusion Detection System, Cloud Computing, Software-as-a-service, Malicious.

I. INTRODUCTION

Historically, an intrusion detection system (IDS) is a proactive monitoring technology and defensive mechanism in protecting critical IT infrastructures from malicious behaviors [1], which may compromise sensitive data and critical applications through cyber attacks. 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 nowadays 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 [2]. In addition, the large capital expenditure required for traditional IT such as needs for training new personnel, licensing new software, etc. can be reduced. Moreover, IDS is commonly deployed in the traditional way, i.e. 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.

A decentralized traditional IDS approach 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 system must be isolated and invisible from the same network where the host and servers reside.

Based on the problems mentioned above, we believe that a proper and economic strategy in IDS implementation is important—with reasonable cost, and reduced complexity with strong defensive mechanism. Thus, we propose an intrusion detection framework based on Cloud services called Cloud-based Intrusion Detection Services (CBIDS) that not only for commercial solution, but also for open research communities. Traffic at different points of the network is sniffed and the interested packets would be transferred to the CBIDS for further inspection. The CBIDS 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.

The paper is organized as follows: in Section II, basic concepts of Cloud computing are discussed. This is followed by classical dedicated IDS and Cloud computing in Section III. Related works of this field are discussed in Section IV. We describe the proposed framework in Section V, followed with discussion in Section VI. Finally, the conclusion and future work are presented in Section VII.

II. INTRUSION DETECTION SYSTEMS

IDS usually monitor, collect and analyze logs, network traffic and user action in a process to identifying suspicious behavior [3]. An IDS is capable of sending early alarm upon risks of exposure caused by any attack. This is to alert the system administrators to execute corresponding response measurements, thus reducing the possibility of serious damage to the system. An IDS is composed of several components such as a sensor which generates security events, a console to monitor events, alerts and control the sensor, and a central engine that's records event logged by the sensor in a database and generates alert from security

978-1-4673-1677-4

event received. Based on the protected objective, IDSs can be classified into host-based IDSs to monitors specific host machines, network-based IDSs to identify attacks occurring in the network and distributed IDSs which combine both host-based as well as network-based IDSs [4]. Based on techniques applied, IDSs can be identified by two techniques, namely misuse, or signature-based detection and anomaly detection [5,6]. Misuse detection techniques can detect known attacks by examining attack patterns, matching them to the list of signatures, much like virus detection by an antivirus application. However, this type of IDS requires frequent updating of the signature database with new signatures; otherwise, it fails to detect unknown attacks if the signature is not in its library. Unlike signature-based detection, anomaly-based detection is designed to capture any activities which deviates from the normal usage pattern/profile, and will be considered as intrusion. Although anomaly detection has the capability to detect unknown attacks, it has the potential to generate high volume of false alarms.

III. CLOUD COMPUTING

Cloud computing is becoming one of the fast developing technologies in computing world. It is builds upon advance virtualization technologies and internet-based computing, where the provider provides infrastructure, platform and software as services (IaaS, PaaS, SaaS) to customers, based on demands [4]. Many practitioners in the commercial and academic spheres have attempted to define exactly what "Cloud Computing" is and what unique characteristics it presents. The National Institute of Standards and Technology (NIST) defines Cloud Computing as ". . . a pay-per-use model for enabling available, 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."

There are three important layers in Cloud architecture: the system layer, the platform layer, and the application layer [7].

The System Layer: The lowest layer in Cloud architecture is the system layer which consists virtualized hosts and networks. Usually, the services delivered at this layer are referred to as Infrastructure-as-a-Service (IaaS).
The Platform Layer: This layer contains virtualized operating systems as well as runtimes and APIs, and the second layer in the architecture. Services delivered at this layer is referred to as Platform as a Service (PaaS).
The Application Layer: The application layer is the top level of the architecture and provides virtual applications. Services delivered at this layer is referred to as Software as a Service (SaaS).

There are some features applied to Cloud computing which motivate users to migrate to Clouds and deploy its services, among those are [7]:

Self-Service: Cloud users' expectation to utilize the on-demand resources immediately. Thus, the Cloud provider must allow self-service access so that users can request, customize, pay, and use the services without intervention of human operators.
Elasticity: Early pictures of Cloud computing where infinite resources can be reached on user claims. Therefore users expect Clouds to rapidly provide resources in any quantity at any time.
Massive scalability: Cloud computing has capabilities to massively scale bandwidth and storage space to accommodate even hundreds or thousands of users' systems.

Naturally, for business reasons, Cloud providers will not reveal their security mechanism details, especially to their competitors. This means that they can even hide any security weaknesses of their system for the sake of their image and reputation. Therefore, not even the users are privy to the details, and they have to rely on the provider to 'take care' of their security concerns and ensure their data are secure and well-protected, especially when the entire data and processes are held in multi-tenant environment as in the Cloud.

IV. RELATED WORK

Basically, IDS involves a determining process on which the behavior of the entity is examined to determine the validity of activities which are hereditary by an entity. A safeguarding architecture which is capable of detecting suspicious attack in distributed computing has been proposed [8], where a single controller is deployed to manage some mini IDS instances that are allocated for each Cloud user and Cloud provider. Machine learning approach and signature based method has been used in this architecture. A successful attack on the network will cause potential impact for multiple users, particularly in Cloud computing. Therefore, concern on network security is foremost today.

IDS development underpins and enables security on the virtualization computing such as Clouds which introduce novel challenges and requires dedicated solution [9]. Communication between multiple virtual machines with the outside world must be monitored. The information which are available in VMM (Virtual Machine Monitor) level can be used by the IDS to detect intrusion correctly. This type of host-based intrusion detection is called VMM-Based IDS, where the IDS resides on physical host machine [10]. However, this type of development seems to bring some additional work and difficulties to the user in terms of cost, knowledge and time.

Many services provided through Cloud are publicly available, and some may be offered by providers who may not the trustable to the users, i.e. users cannot verify whether the provider is from a trusted domain. This weakness exposes users to malicious or intrusion attacks. Thus, an IDS is needed as information filter to provide a strong security defense. Furthermore, IDS can protect Cloud based system from various types of attacks [11]. The advantage of IDS to generate alerts log can help the user to manage their Clouds globally. Cloud providers can deploy IDS which can inspect packets to detect novel attacks that exploit bugs in software at a small cost and must inform user in the occurrence of serious attacks [12].

Traditional IDS deployment is single threaded and not very efficient to handle dynamic and distributed environment such as Clouds which contains enormous network data. Thus, Gul and Hussain [4] gives emphasis of multithreaded IDS deployment in Cloud computing environment. In addition, it is also suggested that Cloud users to purchase third party monitoring service with a frequent alerting mechanism.

Most research carried out recently focus on virtual machine, data and host protection and not enough attention on the overall Cloud network security that is easily exposed to security risks such as phishing attacks, malware, spam and so forth [13].

V. CLOUD-BASED INTRUSION DETECTION SERVICE FRAMEWORK (CBIDS)

Distributed environment such as Cloud computing are the most targetable place to launched cyber attacks for any organization [13]. An IDS which can support scalable and virtualized environment is required to protect public and private Clouds.

Security as a service in distributed environment is not a new trend [13], but current approaches related to Cloud based IDS is rarely explored. Moreover, to the best of our knowledge, the absence of a basic framework as a source of reference and guideline further complicate and hinder any research to introduce IDS as a service in Cloud computing.

We present intrusion detection as a service that monitors Cloud networks for detecting malicious activity. Apart from securing user's critical applications and data, the other principle of Cloud-based intrusion detection service (CBIDS) is to eliminate the need of training new personnel, licensing new software, purchasing hardware, etc. Cloud users are capable to get opportunities and responsibility to administrate IDS which brings more reliable feeling to them through CBIDS framework.

CBIDS framework consists of three principal components; namely, User Data Collector (UDC), Cloud Service Component (CSC), and Cloud Intrusion Detection Component (CIDC). Communication among UDC and CSC which contains confidential information for forwarding purposes is encrypted. We will first present an overview of the CIDBS framework as illustrated in Fig.1 and later discuss each component of the framework in section IV.

User Data Collector (UDC)

The UDC is a secured independent server which contains collection of necessary information. UDC is integrated inside the user Clouds based on user requirements to protect the whole network efficiently. UDC is responsible to standardize and filtered the collection of packets information before being forwarded to Cloud IDS through a secure VPN connection.

Cloud Service Component (CSC)

CSC is in charge of analyzing and validating the received information from UDC to figure out external intrusion before determining whether to delete these information or forward them to appropriate analysis engine inside the Cloud Intrusion Detection Component (CIDC). CSC is also responsible for translating the received information into a common format which is understood by the CIDC.

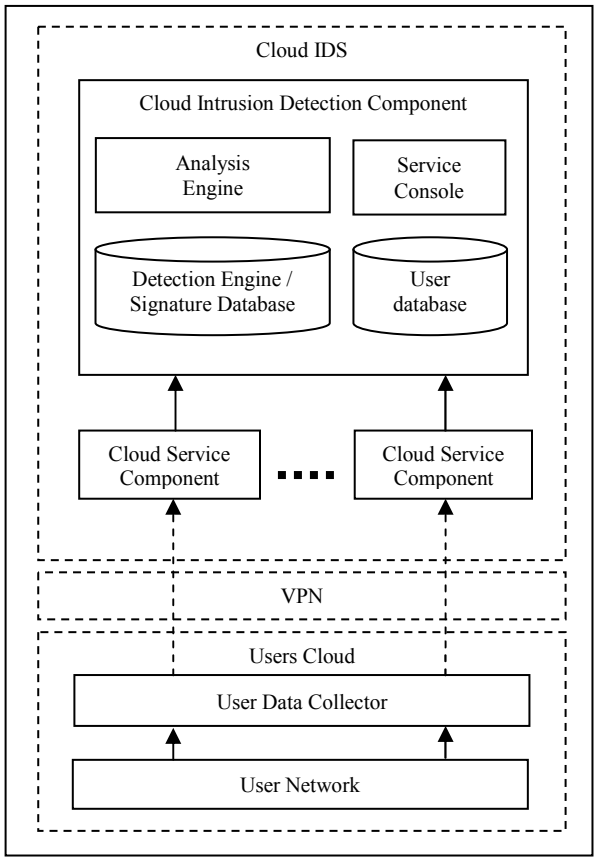

Figure 1. Cloud-based Intrusion Detection Service Framework

Cloud Intrusion Detection Component (CIDC)

CIDC is considered as the principal component for intrusion detection. There are four important modules in CIDC; namely, the Analysis Engine, Service Console, Signature Database and User Database.

Analysis Engine (AE)

AE works as a pattern matching mechanism. It is responsible for data analysis process which came from CSC and matches the data with patterns stored in the signature database. AE is an independent process which can be any IDS, e.g. Snort. AE identifies intrusion activities and generates alerts through the service console.

Service Console (SC)

SC is the remote user preferred service controller. CIDC can be configured for fine tuning based on user demands through SC. SC also handle the user authentication which has privileged access to CIDC. Malicious activities will be reported to the user through SC. Usually, IDS alerts are in different formats, and SC represents all the alerts in a common format called Intrusion Detection Message Exchange Format (IDMEF).

Signature Database (SDB)

SDB contains the entire up-to-date attack signatures.

User Database (UDB)

UDB contains user information such as login information, user activities, etc.

Figure 2. represents the sample scenario architecture based on CBIDS framework. We target Small and Medium Enterprises (SMEs) as the client (Users). The user should fulfill some requirements in order to use CBIDS. An intermediate server (proxy), VPN, virtual switch connection should be allocated on the user network. The illustrated figure comprises into two parts namely Users Cloud and Cloud IDS. The Users Cloud itself contains virtual switches, hosts, and servers which are connected through a virtual network. Several servers and hosts can be created inside the Users Cloud.

In this work, we assume each single machine as a Host-VM. Each Host-VM is connected to virtual switches which support SPAN features. Sensitive information for inbound and outbound traffic of each Host-VM is copied and forwarded to the UDC (proxy). Later, the UDC gathers this information and forwards it to the Cloud CSC (proxy) which resides in the IDS Cloud through a secure VPN connection. The IDS Cloud provides a comprehensive global defensive mechanism and detects the entire attacks based on the information forwarded by the user in real time.

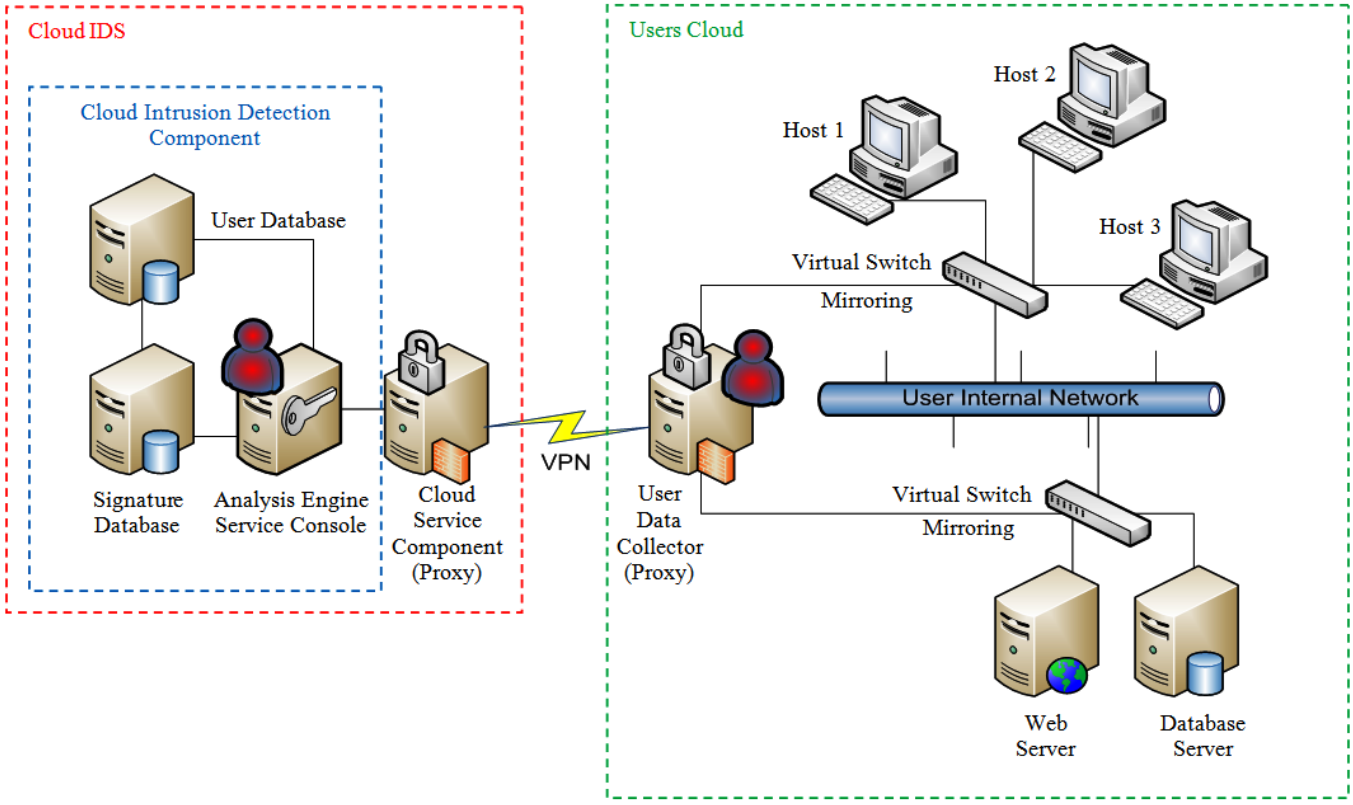

Figure 2. CBIDS sample architecture

When the packets arrive at the CSC, the CSC will proceed to verify and filter the entire information before forwarding the necessary and appropriate information to the AE. The AE matches the appropriate information with the attack signatures stored in the signature database (SDB). After the analyzing process, the AE will produce a report or event to the UC for the user's attention and further action. Users are also provided with specific access into the Cloud IDS through a web-enabled service (UC) to configure and update their service requirements.

VI. DISCUSSION

CBIDS provide an ease of deployment where the user do not need to modify their virtual machines and operating system completely. Thus, the private and public Clouds can be deployed with minimal effort, scalable and flexible, where the virtual machines can be dynamically added and removed. In addition, communications between the Host-VM to internal nodes and Host-VM to external nodes can be observed directly by CBIDS. Modern advance technologies such as virtual switches enable promiscuous mode features and allowing the Cloud users to sniff and forward the traffic to CBIDS.

We isolate the proxy server from the others using independent virtual network and switch features. This will protect the proxy server from being hacked or compromised. For instance, if the proxy server location has been identified by the attackers, soon the attacker can steal all sensitive information and attack the entire host network. Normally, it is easy to attack a server which must accept a request from any users, which will be a target for attackers to launch attacks. The attackers can target an IDS machine or any related machine which acts as an IDS system to render it fail to function or to terminate IDS processes which can be used to detect their activities. Thus in our approach, we isolate and create an independent network connection between the proxy and host using a one-way-communication virtual switch.

In some cases, such as in traditional based IDS deployment, the IDS needs to update patches for every IDS machines. In our concept, the updating processes for the IDS machines are taken care of by the Cloud expertise without any user involvement.

As illustrated in Fig.2, the entire host-VM is connected without using physical network but with virtual network instead, where no extra hardware is needed to construct and implement the virtual environment. User needs to purchase virtualization software which supports the creation of a virtual environment. This eliminates the needs for additional ports, switches, cables, etc.

CIDBS protects users from any kind of serious attacks; even if any one of the host-VM has been compromised the proxy server can still keep receiving network packets through the virtual switch and can continue to forward all information to the Cloud IDS to perform intrusion detection. Later, the user can easily detect the infected host-VM. Based on Figure 2, any access to file system, processes and applications inside the proxy server is prohibited when the virtual switch denies access from any host-VM to the proxy server. Therefore, the proxy server is only configured to receive packets from the port mirroring switch but not from any host directly.

In existing frameworks, multiple hosts-VM can share a single IP address and this can result in difficulties to detect the real compromised host-VM. In our case, each host-VM has different IP address to differentiate traffic originating from each host-VM. In addition, an alert will be generated for each user action. For instance, if the user configures, updates and changes something inside the CBIDS, an alert for each user action will be sent through the user console, email and any other user preferred medium option.

In our framework, the principal idea is to detect an attack in user networks. Various types of operating systems and processes run in user networks have been compromised with new types of attacks every day. Thus, the signatures inside the database are dynamically updated. CBIDS allow users to create their own preferred attack signatures instead of Cloud expertise who are manages the attack signature database in CBIDS. Furthermore, users have the absolute power and option to choose which information they want to forward to the Cloud IDS. In general, CBIDS operates in a trusted domain, which must communicate with users' server through a VPN connection. Each user has secure login to access the User Controller component. They need to get validation as legitimate user to configure their preferred services as they wish.

VII. CONCLUSION

The proposed framework is fundamentally different from the traditional IDS deployment and envisaged to form on Cloud which opens a new era in Cloud computing security. We introduce CBIDS that is capable of detecting all possible threats in public and private Clouds. CBIDS normally receives information from the users and matches the information with signatures in the database. The analysis engine generates alert whenever suspicious content is detected and notifies the user through the user console. The framework offers opportunities for future research in introducing intrusion prevention systems and antivirus as a service in Cloud computing environment.

The proposed framework is described from a solely theoretical perspective. Environments which consist of this framework are work in progress.

REFERENCES

[1] M.N. Doan and H. Eui-Nam, "A Collaborative Intrusion Detection System Framework for Cloud Computing", *Lecture Notes in Electrical Engineering*, Vol. 120, Part 2, pp. 91-109, 2012.

[2] S. Subashini,V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing", *Journal of Network and Computer Applications*, Vol. 34(1), pp. 1-11, 2011.

[3] Z. Muda, W. Yassin, M.N. Sulaiman, N.I. Udzir, "A K-means and Naive Bayes Learning Approach for Better Intrusion Detection", *Information Technology Journal*, Vol. 10(3), pp.648-655, 2011.

[4] I. Gul, M. Hussain, "Distributed Cloud Intrusion Detection Model", *International Journal of Advanced Science and Technology*, Vol. 34, pp. 71-82, 2011.

[5] Z. Muda,W. Yassin,M.N. Sulaiman, N.I. Udzir, "Intrusion Detection Based on K-Means Clustering and Naïve Bayes Classification", In *7th Information Technology in Asia International Conference*, pp.1-6, 2011.

[6] Z. Muda,W. Yassin, M.N. Sulaiman, N.I. Udzir, "Intrusion Detection Based on K-Means Clustering and OneR Classification", In *7th Information Assurance and Security International Conference*, pp.192-197, 2011.

[7] S. Marston, L. Zhi, S. Bandyopadhyay, A. Ghalsasi, "Cloud Computing - The Business Perspective", In *44th Hawaii International Conference on System Sciences*, pp.1-11, 2011.

[8] S. N. Dhage, B. B. Meshram, R. Rawat, S. Padawe, M. Paingaokar, A. Misra, "Intrusion Detection System in Cloud Computing Environment", In *11th Proceedings of the International Conference & Workshop on Emerging Trends in Technology*, pp. 235-239, 2011.

[9] J. Arshad, P. Townend, J. Xu, "A Novel Intrusion Severity Analysis Approach for Clouds", *International Journal of Future Generation Computer Systems*, to be published.

[10] F. Azmandian, M. Moffie, M. Alshawabkeh, J.G. Dy, J.A. Aslam, D.R. Kaeli, "Virtual Machine Monitor-Based Lightweight Intrusion Detection", *Operating Systems Review*, Vol. 45(2), pp.38-53, 2011.

[11] J.H. Lee, M.W. Park, J.H. Eom, T.M. Chung, "Multi-level Intrusion Detection System and Log Management in Cloud Computing", In *13th International Conference on Advanced Communication Technology*, pp.552-555, 2011.

[12] E. Keller, J. Szefer, J. Rexford, R. B. Lee, "NoHype: Virtualized Cloud Infrastructure Without the Virtualization", In *37th annual international symposium on Computer architecture*, Vol. 38(3), pp. 350-361, 2010.

[13] M. Hussain, H. Abdulsalam, "SECaaS: Security as a Service for Cloud-based Applications", In *2nd Kuwait Conference on e-Services and e-Systems*, pp.1-4, 2011.