Journal of Theoretical and Applied Information Technology
10th December 2014. Vol.70 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

COOPERATIVE INTRUSION DETECTION SYSTEM FRAMEWORK USING MOBILE AGENTS FOR CLOUD COMPUTING

[1]HICHAM TOUMI, [2]AHMED EDDAOUI, [3]MOHAMED TALEA

[1,3]Information Processing Laboratory, Department of Physical, University Hassan II Casablanca, Morocco

[2]Department of Mathematics and Computer Science, University Hassan II, Casablanca, Morocco

E-mail: [1]toumi.doc@gmail.com,[2]ahmed_eddaoui@yahoo.fr,[3]taleamohamed@yahoo.fr

ABSTRACT

Cloud computing improves collaboration, flexibility, scaling, and availability, and provides the potential for cost reduction through optimized and efficient computing. Cloud computing allows the use of a collection of services, applications, information, and infrastructure composed of group of compute, network, information, and storage resources. In brief, the Cloud Computing is undergoing an incontestable success, which could be indeed compromised by concerns about the risks related to potential misuse of this model aimed at conducting illegal activities. To address these problems, a framework of cooperative Hybrid intrusion detection system (Hy-IDS) and Mobile Agents is proposed. This framework allows protection against the intrusion attacks. Our Hybrid IDS is based on two types of IDS, the first for the detection of attacks at the level of virtual machines (VMs), the second for the network attack detection and Mobile Agents. After the collection of malicious data from infected sources (VMs) via the first category of IDS; the second category of IDS is also used for the generation of new signatures from the collected data based on a signature generation algorithm. However, these new signatures are used to update the database of the IDS itself. The mobile agents play an important role in this collaboration. They are used in our framework for investigation of Hosts, transfer data malicious and transfer update of a database of neighboring IDS in the cloud. With this technique, the neighboring IDS will use these new signatures to protect their area of control against the same type of attack. By this type of close-loop control, the collaborative network security management system can identify and address new distributed attacks more quickly and effectively.

In this paper, the existing IDS and Mobile Agents technology are studied. Then we develop a collaborative approach based on Hy-IDS and Mobile Agents in Cloud Environment, to define a dynamic context which enables the detection of new attacks.

Keywords: Cloud Computing**,** *Hy-IDS, Mobile Agents, Collaborative, Signatures.*

1. INTRODUCTION

Cloud computing is an evolving concept that describes the development of many existing technologies and approaches to computing into something different. Cloud is the delivery of computing services over the Internet. Cloud services allow individuals and enterprises to use software and hardware that are managed by providers at remote locations. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Also, it provides a shared pool of resources, including data storage space, networks and computer processing power. These components can be rapidly deployed, provisioned, implemented, and scaled up or down. It provides a model of allocation and consumption on demand. Cloud enhances collaboration, flexibility, scaling, and availability, and provides the potential for cost reduction through optimized and efficient computing. At the same time, the transformational nature of the cloud is associated with significant security and privacy risks.

The fast growth of cloud computing technology introduces more of the vulnerabilities. Security is considered to be one of the most critical aspects in cloud computing environment due to the confidential and important information stored in the cloud. Network security appliances, such as IDS and NIDS are widely deployed in advantage points and play an important role in protecting the network from attacks. Most of these appliances work

Journal of Theoretical and Applied Information Technology
10th December 2014. Vol.70 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

without collaboration, their detection results are isolated, and cannot be collected and analyzed systematically. Therefore, we thought of a new security policy that allows the detection of distributed attacks such as deny of service (DoS) and Distributed Denial of Service (DDoS).

In this paper, we present a new approach of collaborating Hybrid Intrusion Detection System (Hy-IDS) and Mobiles Agents in Cloud (offering IaaS). Our Hy-IDS based on two types of IDS; then this collaboration allows to the first type IDS which use mobile agents to collect evidences of an attack from all the attacked VM for further analysis and auditing. Moreover, after the detection of attacks by the first type of IDS this last notified second type of IDS by transfer mobile agents for generate new signatures. Finally, the new signatures will be used to update the database IDS belonging to the neighboring domain under the direction of a cloud administrator.

The rest of this paper is organized as follows: The section II presents theoretical background and discusses some related works in the area of Mobile Agent-based IDS and NIDS. The section III forms the core of this paper explains and describes in detail our approach. Whereas the proposed framework is discussed in section IV; finally we give conclusion, perspective and references in section V.

2. THEORETICAL BACKGROUND AND RELATED WORK

The rest of this section is organized as follows: we start with theoretical background as the first part and Related Work as a second part.

2.1 Cloud Computing

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is provides dynamically scalable and virtualized resources as services over the Internet. It uses virtualization, service-oriented software, and grid-computing technologies, among others. Cloud computing allows accessing resources and services offered by servers from different places. Therefore, it is a model of distributed computing [1].

NIST defines cloud computing by describing five essential characteristics, three cloud service models, and four cloud deployment models. They are summarized in visual form in figure 1 and explained in detail below [2].

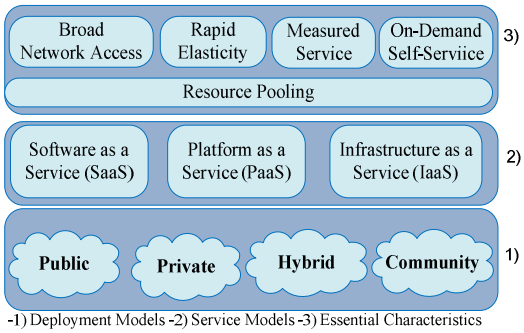

Figure 1: Visual Model of Cloud Computing Definition

2.1.1 Cloud computing characteristics

Cloud services exhibit five essential characteristics that demonstrate their relation to, and differences from, traditional computing approaches:

On-Demand Self-Service: A user can unilaterally provision computing capabilities such as server time and network storage as needed automatically, without requiring human interaction with a service provider.

Broad Network Access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms as well as other traditional or cloud-based software services.

Resource Pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid Elasticity: Rapid elasticity is a cloud computing term for scalable provisioning, or the ability to provide scalable services. To the user, the capabilities available for provisioning often seem to be unlimited and can be purchased in any quantity at any time.

Measured Service: Cloud resource usage can be measured, controlled and reported providing transparency for both the provider and the user of the utilized service (e.g., storage, processing, bandwidth, or active user accounts). This is crucial for billing, access control, resource optimization and other tasks.

Journal of Theoretical and Applied Information Technology
10th December 2014. Vol.70 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.1.2 Cloud service models

The providers of cloud distinguish three services of cloud computing.

Software as a Service (SaaS): SaaS software is used directly on the network, without being downloaded first in the local computer user environments. The software applications are available on the Internet via a SaaS provider, and are executed in the computing environment predefined from this supplier [3]. Cloud computing present elasticity, signifying your resources and costs can increase or decrease with your demands. SaaS usually involves a set fee per user, per month, so costs and the functionality offered tend to be fixed.

Infrastructure as a Service (IaaS): Iaas provisions hardware, software, and equipments (mostly at the unified resource layer, but can also include part of the fabric layer) to deliver software application environments with a resource usage-based pricing model [4]. A cloud provider providing IaaS can rent fundamental infrastructures which include computing resources and storing data to user. IaaS provider may add or remove computing or storage resources instantly when demanded by user.

Platform as a Service (PaaS): PaaS is a computing environment available and accessible, as needed, over network from a service provider. Used to develop and run software [5]. The user may use programming languages and tools supported by the provider's platform to construct their own application in more efficient manner.

2.1.3 Cloud deployment models

We distinguish three types of cloud computing: the public cloud, private cloud and hybrid cloud is actually a combination the first two (Figure 2).

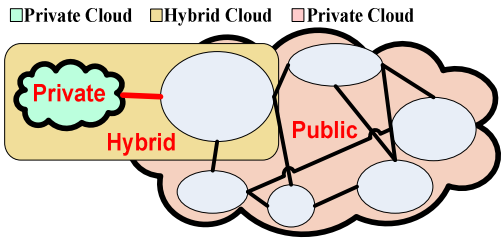

Figure 2: Types of Cloud Computing

Public Cloud: The cloud infrastructure is made available to the general public or a large industry group and is establishment by an organization selling cloud services. When a Cloud is made available in a pay-as-you-go manner to the general public, we call it a Public Cloud [6]. Providers of the most popular public cloud are Google and Amazon.

Private Cloud: Also presented to as internal cloud or on-premise cloud. In a private cloud only the consumers, who belong to the same organization that owns the cloud and have the access to its resources can access service [6]. In addition, a private cloud is designed to provide the same features and benefits of public cloud systems, but removes a number of objections to the cloud computing model.

Hybrid cloud: "This cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)" [7]. The growing importance of hybrid cloud environments is transforming the entire computing industry as well as the way enterprises are able to leverage technology to innovate.

Community Cloud: Community cloud. Several organizations jointly construct and share the same cloud infrastructure as well as policies, requirements, values, and concerns [8]. Community clouds are a subset of public clouds customized to a specific vertical industry that offer a variety of services including Software as a Service (SaaS), Business as a Service (BaaS) or Platform as a Service (PaaS).

Cloud computing is a new large-scale distributed computing model. Virtualization, instantaneous deployment, broadband networks and other key technologies are applied in the cloud computing. It realizes intercommunication, interconnection through Internet. In the form of a unified service, cloud computing uses the multi-terminal, multi-platform, multi-network for users to access a pay-as-you-go, dynamic configuration, flexibility expansion, low cost, high availability service by the standard browser at any time and any place. The services include computing, storage, resource, and platform and so on. Cloud computing provides efficient solutions which to meet the demand of rapid increase of hardware cost, calculation storage capacity, services computing and the development of Web3.0. It more and more receives the attention of government, enterprises and research institutions [9]. At the same time, the transformational nature of the cloud is associated with significant security and privacy risks.

Journal of Theoretical and Applied Information Technology
10th December 2014. Vol.70 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.2 Intrusion Detection Systems (IDS)

It becomes crucial part in the Cloud computing environment. The main aim of IDS is to detect computer attacks and provide the proper response [13]. An IDS is defined as the technique that is used to detect and respond to intrusion activities from malicious host or network [14].

The Intrusion Detection Service (IDS) increases a Cloud's security level by providing two methods of intrusion detection. First method is behavior-based method which dictates how to compare recent user actions to the usual behavior. The second approach is knowledge-based method that detects known trails left by attacks or certain sequences of actions from a user who might represent an attack. The audited data is sent to the IDS service core, which analyzes the behavior using artificial intelligence to detect deviations. This has two subsystems namely analyzer system and alert system. In order to detect the intruders the following techniques should be implemented in either HIDS or NIDS [15] [14] [16].

2.2.1 NIDS in the cloud: existing approaches

In [17] for improving IDS performance the authors proposed an efficient model that used multithreading technique in Cloud environment to handle large number of data packet flows. The proposed multi-threaded NIDS is based on three modules named: capture module, analysis module and reporting module. The first one is charged of capturing data packets and sending them to analysis part which analyzes them efficiently through matching against pre-defined set of rules and distinguishes the bad packets to generate alerts. Finally, the reporting module can interpret alerts and immediately make alert report.

2.2.2 Traditional NIDS uses signature based and anomaly detection techniques.

A-Signature based detection: Signature based detection defines a set of predefined rules used to decide that a given pattern is that of an intruder. Signature based systems are able of attaining high levels of accuracy and minimal number of false positives in identifying intrusions. In Cloud, the signature based detection technique can be used to detect external intrusions at the front end or to detect external/internal intrusions at the back end. But, it has the disadvantage; this technique fails to detect the unknown attacks.

B-Anomaly detection: It necessitates the collection of data relating to the behavior of legitimate use over a period, and then applies statistical tests to the observed behavior, which determines whether that behavior is legitimate or not. It has the advantage of detecting unknown attacks. Anomaly detection technique can be used for Cloud to detect unknown attacks at different layers. However, large numbers of network level events makes difficult to monitor or control intrusions using anomaly detection technique in the Cloud [10].

2.2.3 Essential characteristics of NIDS

NIDS must have the following characteristics for integrating it in the cloud computing.

- Detection of network attacks on each layer

NIDS must be able of detecting intrusions at each component like front end and back end. It should be capable to detect known attacks as well as unknown attacks.

- Faster detection rate

High number of users is concerned in cloud. So, this number may turn into high traffic rate in Cloud. Therefore, NIDS must have faster detection at lower cost.

2.3 Signature Generation Algorithm

To prevent systems from new attacks, the IDS should be quickly updated. However attacker instead of finding new types of attack tries to remain unnoticed in the evading system by using signature. If we take one of the types of IDS as NIDS; then, for real time evasion IDS (e.g., NIDS) is created using the signature generation algorithm (e.g., Apriori Algorithm, Signature Apriori Algorithm). The aim of evasion is not to break the NIDS system but to make system sturdier. Different sessions of attacks are given as input to the signature generation algorithm. According to support and confidence value rule is generated by the signature generation algorithm. These rules are given to NIDS. When an attack is generated for which signature is stored in database NIDS, it generates an alarm. If NIDS failed to generate alarm means evasion is successful. So we found out different types of evasion [18].

2.4 Relevant Works and Limitations

In the literature there are few works that use IDS, NIDS (Snort and signature apriori algorithm) and mobile agents in the cloud computing. In this section, we present three works, the first work is based on Snort combined with a signature apriori algorithm, the second work is based on IDS and mobile agents; finally a work that is based on mobile agents.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The first work presented by Chirag N. Modi et al, combine Snort (Snort-Home page N.d.) and signature apriori algorithm in their NIDS module. The objective of this approach is to reduce impact of network attacks (known attacks as well as derivative of known attacks). The network may be external network or internal network. Snort will monitor those network packets and allow/deny them based on the configured rules. Also, captured packets, partially known attack signatures (stored in known signature database) and support threshold are given as input to the signature apriori algorithm. Using given input, signature apriori generates new possible signatures and updates them as rules in Snort. So, derivative attacks can be detected by Snort [10].

But this work is unable to detect intrusion at the hosts, and Distributed denial of service attacks (DDOS).

The second work, A.V. Dastjerdi et al. they tried to offer a line of defense by applying Mobile Agents technology to provide intrusion detection for Cloud applications regardless of their locations. These researchers build up a robust distributed hybrid model scalable, flexible and cost effective method based on mobile agents (MA). VMs are attached to MA which collects evidences of an attack from all the attacked VMs for further analysis and auditing. Then, they have to correlate and aggregate that data to detect distributed attacks [11].

This kind of work is limited to the detection of attacks at machines. They did not think to monitor network traffic simultaneously.

The third work is essentially the proposal of an architecture that can respond to user needs through access to a cloud computing secure with mobile agents. A. Alwesabi et al. they are relying on the ability of mobility and security agents. Their architecture is based on mobile agents that have kept the goal of communication in security in cloud computing. The concept of mobile agent appears in this context as a solution to facilitate the implementation of dynamically adaptable applications, and provides a generic framework for the development of cloud computing applications [12]. But, they did not exploit mobile agents for security against intrusion attacks.

After a thorough study of various security policies, we found the need for collaboration of several security policies. This collaboration is mainly based on mobile agents. Then we exploit mobile agents for security against intrusion attacks and at the same time as a communication tool between different layer of cloud computing. For this reason, we combine between the strengths of these previous works in our approach. We will argue in the next section that this collaboration has several advantages.

3. OUR APPROACH

In this section are first presented the objectives of the proposed system, its overall architecture, highlighting its four main layers and overall functioning.

3.1 The Objectives of the Framework

The proposed framework could reduce the impact of several types of attacks. The architecture proposed in our work is a mobile agent based approach conceived for the execution of a service in cloud (IaaS). Also, it defines a set of functional modules described in terms of their behavior, interfaces and components (Mobile Agents, Intrusion Detection System, and Signature Generation Algorithm). Then, it defines how these components interact in order to accomplish all the tasks correctly in the system.

The objectives of our framework are grouped into three main Points as follows:

I. Intrusion detection in virtual machines using mobile agents. We use IDS-C that based on combined IDS with the living environment of mobile agents; it uses mobile agents for collecting evidences of attack from all the attacked VM for further analysis and auditing. In case of attack, IDS-C aggregate malicious data, then placing them in a temporary database.

II. Generating new signatures from malicious data, which were collected in the first part. We use as the second part IDS-Cr that consists of a (IDS and Signature Generation Algorithm); it uses Mobile Agents for aggregation and collection of malicious data from the lowest layer (temporary database). Then IDS-Cr uses all malicious data collected from different IDS-C (each IDS-C contains a temporary database) and using them to generate new signatures through a Signature generation algorithm.

III. We used the newest signatures for update the database IDS-Cr, this IDS-Cr may be belonging to the domain that created new signatures or belong to the neighboring domain.

Journal of Theoretical and Applied Information Technology
10th December 2014. Vol.70 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.2 Our Proposed Hybrid Framework

3.2.1 Components of our framework

In figure 3, our Hybrid Intrusion Detection System (Hy-IDS) combines Intrusion Detection System Center (IDS-Cr), Intrusion Detection System Control (IDS-C) and Intrusion Detection System Master (IDS-M). The IDS-Cr consists of an Intrusion Detection System (IDS) and Signature Generation Algorithm (SGA); IDS-C based on combined IDS with the living environment of mobile agents named Agents Agency (AA). The IDS-M is based on Intrusion Detection System (IDS) and Living Environment of Mobile Agents named Agents Agency (AA). Concerning the types of IDS; there are network based (NIDS) and host based (HIDS) intrusion detection systems. Then, some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system.

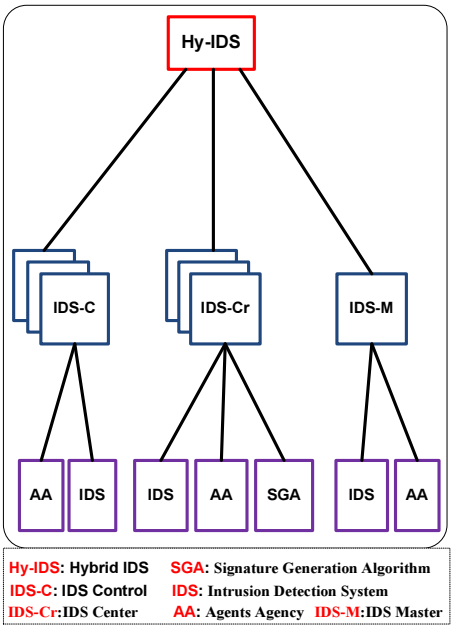

Figure 3: Components of our Hy-IDS

Finally, using mobile agents to ensure communication between the IDS-C, IDS-Cr and IDS-M.

- **IDS**

IDS have the ability to perform real-time traffic analysis and packet logging. IDS perform protocol analysis, content searching and content matching. It comprises of multiple components that communicate with each other in order to detect intrusion according to its signature database. It is configurable and constantly updated.

- **Signature Generation Algorithm**

Different sessions of attacks are given as input to Signature Generation Algorithm (e.g, Apriori Algorithm and Signature Apriori Algorithm). According to support and confidence value rule are generated by Signature Generation Algorithm. These rules are given to IDS. When attack is generated for which signature is stored in IDS, it generate alarm.

- **Agents Agency**

Agency presents an environment for mobile agents to become alive. An agency is responsible for hosting and executing Agents in parallel and provides them with environment so that they can access services, communicate with each other, and migrate to other agencies. Also, an agency protects the underlying VMs from unauthorized access by malicious Agents.

3.2.2 Architecture of our cloud computing

As shown in Figure.4, Cloud is based on a front-end and back-end. Cloud users are able to communicate with Cloud via front end. Front end is connected to both external network as well as internal network. It is presented in the figure 4 by the Cloud layer. Back-end consists of computer hardware and software that are designed for the delivery of services. It allows treatment of the user's query and executes it for allowing to access VM instances. Then, it is presented in the figure 4 by the Cluster-Layer, Node-Layer and VM-Layer.

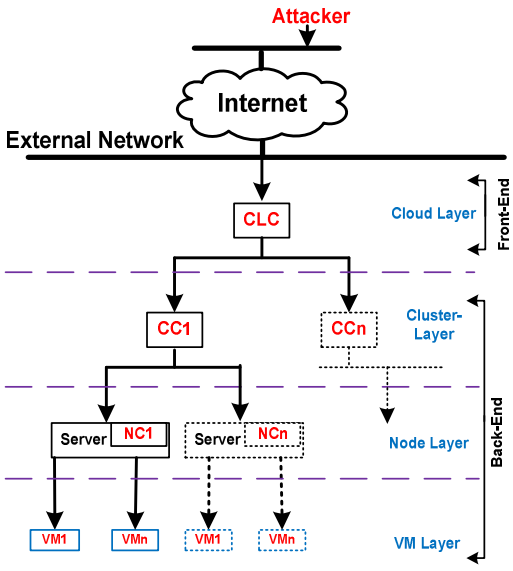

Figure 4: Our cloud computing

Journal of Theoretical and Applied Information Technology
10th December 2014. Vol.70 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The Cloud Controller (CLC) provides EC2-compatible interfaces, as well as a web interface to the outside world. The CLC acts as the administrative interface for cloud management and performs high-level resource scheduling. Only one CLC can exist per cloud and it handles authentication, accounting, reporting.

The Cluster Controller (CC) acts as the front end for a cluster within a cloud computing and communicates with the Cloud Controller and Node Controller. It manages instance (i.e., virtual machines) execution and Service Level Agreements (SLAs) per cluster.

The Node Controller (NC) at level of physical server; it hosts the virtual machine instances and manages the virtual network endpoints. While, there is no theoretical limit to the number of Node Controllers per cluster.

3.3 Building a Solution Framework

Following the presentation of the components of our Hy-IDS and the cloud model proposed in the previous part. We superimposed our Hy-IDS with the cloud computing model in Figure 5.

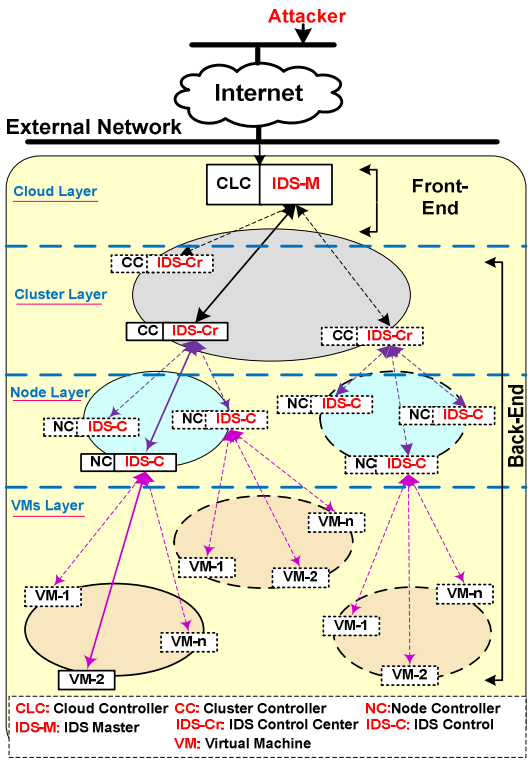

Figure5: The Hierarchy of Our Cloud Computing

We placed IDS-C at the level of nodes (physical server) for monitoring virtual machines. It allows the detection of intrusion and malicious data aggregation using mobile agents. Then, we placed IDS-Cr in the front-end Cluster for the monitoring of nodes. Also, it generates new signatures. Finally we placed IDS-M in the front-end Cloud for the monitoring of Clusters and Management of Update.

3.4 Functioning of Our Framework

The fundamental design of our proposed hybrid model in VM-layer and Node-layer; in which each node consists of three main components namely IDS Control (IDS-C), Agents Agency (living environment of mobile agents), Specific Static Agent Detectors (SA).

Static Agents (SA) placed at the level of virtual machines. It should generate an alert whenever they detect suspicious activities; then send alert's ID to IDS control. Then, IDS Control will send investigative Mobile Agent (IMA) with a specific task, to every agency that sent similar alerts. IMA will visit and investigate all those VMs, collect information, correlate it and finally send or carry back the result to IDS control.

In case of attack, IDS-C aggregate malicious data, then placing them in a temporary database. Then IDS-C uses Transfer Mobile Agents (TMA) for notifying IDS-Cr placed in the cluster layer. Moreover, IDS-Cr dispatches Investigative Mobile Agents (IMA) to any IDS-C those send TMA for aggregation and collection of their malicious data from the database temporarily. Then IDS-Cr uses all malicious data collected by IMA and using them to generate new signatures through a Signature generation algorithm.

Finally, these new signatures will be used to update the database IDS belonging to this IDS-Cr, then the database to IDS belonging of IDS-Cr the cluster neighboring. These updates go through the IDS-M, to maintain a hierarchical structure in our framework. Among the advantages of our approach, other clusters are protected against the same category attack. Our approach consists of the following features:

1) Continuous detection of attacks;

2) Incrementally deployable security elements;

3) Dynamically enable / disable / upgrade security elements.

Mobile agents are by nature autonomous, collaborative, self-organizing, and mobile.

4. DISCUSSION

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Existence of vulnerabilities in Cloud computing allow intruders to affect the confidentiality, availability and integrity of cloud resources as well as services. Detection of DoS/DDoS attack and other network level malicious activities are major security concerns in the Cloud. To address this issue, integration of only firewall, NIDS (Snort and Signature Apriori) [10] or Mobile Agent based intrusion detection system (IDS) [11] in the cloud is not an efficient solution. Our proposed solution framework (cooperative Hybrid intrusion detection system into Cloud) can be used to detect network attacks (known attacks as well as derivative of known attacks) at the front end as well as the back end of Cloud environment (i.e IaaS). It aimed to achieve low false positive alarm rate within reasonable computational cost, the same time resolve the problem of the old insulation solutions.

Moreover, by using Signature Generation Algorithm and the exchange of updates between cluster techniques, then these latter permit to our framework to achieve new knowledge and detect new kind of intrusion. Outstanding scalability is another strong point of our framework. When for example our VM migrates to a machine out of organization boundary (for example from our private Cloud to a public Cloud), it is still possible to perform intrusion detection as our IMA can migrate just like VMs, and the same rule applies to other mobile agents (Transfer Mobile Agents and Mobile Agent Update). And this is strength of our framework which gives the IDS and NIDS great scalability and flexibility. Therefore, we have met almost all the mentioned challenges in our framework.

5. CONCLUSIONS AND FUTURE WORKS

Cloud computing is the new buzz in the computing world. Cloud-computing although present lots of advantages to organizations, also organizations need to carefully understand the security measures provided by the cloud provider for protecting them against the attacks.

The paper proposes an intelligent architecture for integrating Security Policy, it is based on the collaboration of the IDS-C, IDS-Cr, IDS-M and Signature Generation Algorithm; this cooperation is performed through mobile agents. As mentioned previously, mobile agents are used in our model for investigation of Hosts, transfer data malicious, transfer update of a database in the cloud. In order to give them ability of investigation in remote hosts and of communication and communication between hierarchical layers or cluster, they should be granted a permission of accessing the Hosts resources like file system, network interfaces, database, and so on. There are two options, first is to give them every right to access all resources. Also, second is to restrict their access to the resources which they need for investigation [21]. Therefore, IDS-Control and IDS-Control Center should issue a certificate which will authorize a mobile agent to access to certain resources on remote Hosts (e.g. for communication between the IDS-C itself or between IDS-C and IDS-Cr). However, it should be aforementioned that Intrusion detection systems control (IDS-C) and intrusion detection systems control center (IDS-Cr) which use mobile agents take over the beginners of mobile agents toolkits such as security architecture flaws. Consequently, further development of mobile agent's toolboxes will make it easier to enforce them into IDS systems.

Further research can be undertaken to improve the work presented.
That we propose the following:
- We will continue to deepen the concepts and the notions of this architecture and to proceed after to its implementation in order to validate it.
- Take into account the adaptability of agents' appearance.
- Use of cooperation mechanisms between mobile agents in order to effectively perform the tasks required.

REFERENCES

[1] Jean-Henry Morin, Jocelyn Aubert, Benjamin Gateau. "Towards Cloud Computing SLA Risk Management: Issues and Challenges", 45th Hawaii International Conference on System Sciences, 2012.

[2] Amin Jula, Elankovan Sundararajan, Zalinda Othman." Cloud computing service composition: A systematic literature review", Expert Systems with Applications 41 (2014) 3809–3824

[3] Linlin Wu, Saurabh Kumar Garg, Rajkumar Buyya. "SLA-based admission control for a Software-as-a-Service provider in Cloud computing environments" Journal of Computer and System Sciences 78 (2012) 1280–1299.

[4] Sunilkumar S.Manvi, GopalKrishnaShyam." Resource management for Infrastructure as a Service (IaaS) in cloud computing: Asurvey", Journal of Network and Computer Applications 2013.

[5] Jonatha Anselmi, Danilo Ardagna, Mauro Passacantando." Generalized Nash equilibria for SaaS/PaaS Clouds", European Journal of Operational Research 236 (2014) 326–339

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[6] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing", UC Berkeley Reliable Adaptive Distributed Systems Laboratory, February 10, 2009.

[7] P. Mell, T. Grance, "The NIST Definition of Cloud Computing", Jan. 2011, U.S. Department of Commerce.

[8] Tharam Dillon, Chen Wu and Elizabeth Chang. " Cloud Computing: Issues and Challenges", 24th IEEE International Conference on Advanced Information Networking and Applications 2010.

[9] Xing Xu, Hao Hu, Na Hu and Weiqin Ying,"Cloud Task and Virtual Machine Allocation Strategy in Cloud Computing Environment" NCIS 2012

[10] Chirag N. Modi, Dhiren R. Patel, Avi Patel, Muttukrishnan Rajarajan, "Integrating Signature Apriori based Network Intrusion Detection System (NIDS) in Cloud Computing". 2nd International Conference on Communication, Computing & Security (ICCCS-2012), 905 – 912.

[11] Dastjerdi, Amir Vahid, Kamalrulnizam Abu Bakar & Sayed Gholam Hassan Tabatabaei. "Distributed Intrusion Detection in Clouds Using Mobile Agents", In Proceedings of the 2009 Third International Conference on Advanced Engineering Computing and Applications in Sciences. ADVCOMP '09 pp. 175–180, 2009

[12] Alwesabi Ali, Almutewekel Abdullah & Okba Kazar. "Implementation of Cloud Computing Approach Based on Mobile Agents". International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 02– Issue 06, November 2013

[13] U. Thakar, "HoneyAnalyzer – Analysis and Extraction of Intrusion Detection Patterns & Signatures Using Honeypot". The second International Conference on Innovations in Information Technology, Dubai, UAE September 26-28, 2005.

[14] K. V. S. N. R. Rao, A. Pal, and M. R. Patra, "A Service Oriented Architectural Design for Building Intrusion Detection Systems", International Journal of Recent Trends in Engineering, vol. 1, no. 2, pp. 11-14, 2009.

[15] R. Bace and P. Mell, "NIST Special Publication on Intrusion Detection Systems", National Institute of Standards and Technology.

[16]Hassen Mohammed Alsafi, Wafaa Mustafa Abduallah and Al-Sakib Khan Pathan,"IDPS: an integrated intrusion handling model for cloud computing environment". International Journal of Computing & Information Technology (IJCIT), 2012, vol. 4, no 1, p. 1-16.

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

[18] N. B. Dhurpate and L.M.R.J. Lobo; "Network Intrusion Detection Evading System using Frequent Pattern Matching". International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 8- August 2013.

[19] Pradeep Kannadiga and Mohammad Zulkernine School of Computing Queen's University, Kingston Ontario, Canada K7L 3N, DIDMA: A Distributed Intrusion Detection System Using Mobile Agents, 2005 IEEE.

[20] H. Zhengbing, L. Zhitang & W. Jumgi. 2008. A Novel Intrusion Detection System (NIDS) Based on Signature Search of Data Mining. "In WKDD First International Workshop on Knowledge discovery and Data Mining". pp. 10–16.

[21] Amir Vahid Dastjerdi, and Kamalrulnizam Abu Bakar. "A Novel Hybrid Mobile Agent Based Distributed Intrusion Detection System". International Journal of Computer, Information Science and Engineering Vol: 2 No: 9, 2008.