Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Integrated for Security Issues with Possible Solutions in Cloud Computing

Kranthi Kiran G*, V Mallaiah, MD Shabbeer
Asst. Prof., Dept. of CSE, CMR Technical Campus
Telangana, India

Abstract: ***Anomaly Software Agent system, the primary benefit of an Agent-based Information Leakage Detection system lies in the ability to modify and add detection capabilities, modularize those capabilities, and then conditionally employ such We propose an enhanced Dynamic security scheme in SaaS in Clouds using capabilities at the discretion of a central control mechanism (in our system, the Controller Agent). The use of mobile agents as described in this paper, and in general, reduces the per-host administrative complexity as once the initial agent environment is properly installed and configured; all further necessary actions are performed by the agents themselves. Additionally, mobile agents are able to provide unique reporting capabilities that, for the purposes of our research, may benefit the analysis of information leakage, protection and the underlying covert channels through which information has been leaked.***

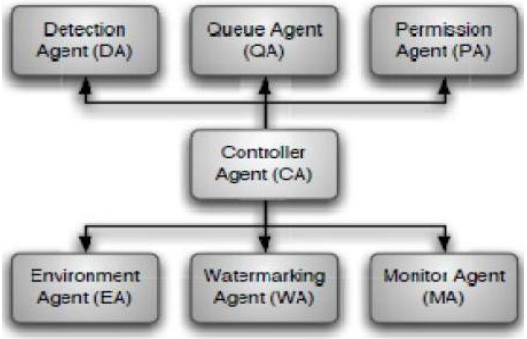
Keywords: ***dynamic protection schema, cloud computing, cloud service***

I. 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 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.



II. 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.

A. 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. 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.

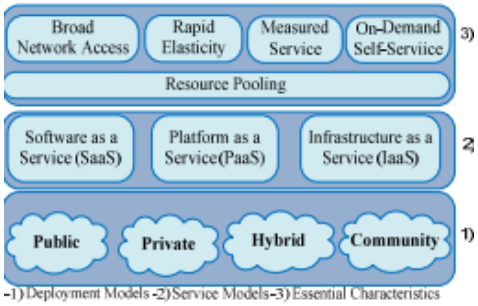


Figure 1: Visual Model of Cloud Computing Definition

B. 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:

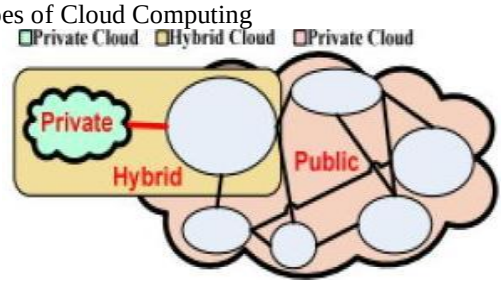
Rapid elasticity is a cloud computing term for scalable provisioning, or the ability to provide scalable services. To the user, the capabilities available for provisioning often seem to be unlimited and can be purchased in any quantity at any time. Measured Service: Cloud resource usage can be measured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

C. 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. Cloud computing present elasticity, signifying your resources and costs can increase or decrease with your demands. SaaS usually involves 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. 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.

D. 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.

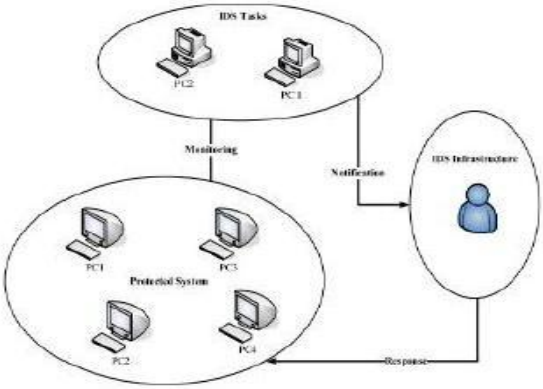
Hybrid cloud: "This cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)" [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, multiplatform, multi-network for users to access a payas-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.

III. 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 [10]. An IDS is defined as the technique that is used to detect and respond to intrusion activities from malicious host or network [11]. 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 [12] [11] [13].



A. NIDS in the cloud: existing approaches

In [14] 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.

B. 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 [15].

C. 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.

IV. 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 [16].

V. 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. 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 [15].

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 [17]. 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 [18]. 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.

VI. CONCLUSION AND FUTURE WORK

In this paper, we introduced cloud specific security problems and the Security Audit as a Service incident detection system, which aims to solve them. To mitigate the shortcomings of traditional intrusion detection systems we showed the advantages of using autonomous agents as a source for sensor information. A first meta model was shown. Since SAaaS agents can be moved business flow dependent to cloud instances during runtime the system acknowledges a cloud flexibility and scalability advantages. It has been shown in several examples, that behaviour monitoring can detect cross customer incidents, which for example can help to limit Denial of Service attacks. An evaluation showed that the selected agent framework is lightweight enough to support a cloud's changing infrastructure and how the SaaS architecture addresses the presented cloud specific security problems.

As for future work, we identified the following tasks:

a) comprehensive research in anomaly detection algorithms,
b) comprehensive research in complex event processing,
c) development of the SSLA policy modeler,
d) development of SAaaS agents.

Additionally, to reduce network load and to avoid event storms the event data could be compressed before sending. This can be done using standard compression algorithms or to gain even higher compression ratios, by aggregating and preprocessing the data to create higher level information (e.g. information about the amount of connections of each host in the last x minutes). Research has to be done how this can be efficiently achieved for different types of data.

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

[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] 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.

[11] 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.

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

[13] 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.

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

[15] 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.

[16] 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.

[17] 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.

[18] 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.

AUTHOR PROFILE

KRANTHI KIRAN G presently working as a Assistant Professor in CMR Technical campus, Hyderabad, Telangana, INDIA. He received his M.Tech (CSE) degree from Sphoorthy Engineering College in the year 2012.He received B.E. (CSE) degree from M.V.S.R Engineering College, in the year 2009. His fields of interests are Cloud Computing, Machine learning, Network Security, etc.

MALLAIAH VANGURI presently working as Assistant professor in CMR TECHICAL CAMPUS, Hyderabad, Telangana, INDIA. He received M.TECH (CSE) form MTIST JNTUH in 2013, B.TECH (CSE) 2005 from TEC in JNTUH. His field of interest is networking.

MD.SHABBEER presently working as an Assistant Professor in CMR Technical campus, Hyderabad, Telangana, INDIA. He received his M.Tech COMPUTER NETWORKS degree. His fields of interests are Networks and Network Security, etc.

