Handling of Intrusions using Genetic Algorithm for Virtualized Environment

Prashant Singh
Department of Computer Science & Engineering
Amity School of Engineering & Technology
Amity University, Lucknow

Bramah Hazela
Department of Computer Science & Engineering
Amity School of Engineering & Technology
Amity University, Lucknow

Abstract

Intrusion detection system (IDS) is all about to detect and prevent the malicious behaviour on the cloud computing. An intrusion detection system which is based on the cloud computing to minimize the risk of intrusions on the cloud networks and cover up the deficiency of already in use intrusion detection systems. Cloud Computing is a newly emerging and lightning fast growing technology. Its popularity reaches to another level day by day due to its amazing services delivery ability. As we all well familiar that distributed nature of cloud computing environment resources, data and applications are quite vulnerable to the attack in cloud environment. Generally in a cloud the data are transferred among the client and the server. During the transferring of the data takes place, security becomes the major concern. An Efficient security mechanism or system must be employed in a cloud in order to make the computing environment fully secure from unauthenticated users. Here, reviewing the one of the most powerful technique in soft computing i.e. Genetic Algorithm which helps in handling the intrusions in virtualized environment.

Keywords: Cloud computing, DDoS, Anomaly, Signature, HIDS, NIDS, Genetic Algorithm

I. INTRODUCTION

Cloud computing is a model for enabling on-demand network access in order to share various computing resources such as network bandwidth, storage, applications, etc[6] . The providers must ensure that they get the security aspects right, for they are the ones who will shoulder the responsibility if things go wrong. The cloud offers several benefits such as quick deployment, pay-for-use, lower costs, scalability, rapid provisioning, rapid elasticity, universal network access, greater resiliency, hypervisor protection against network attacks, low-cost based disaster recovery and data storage solutions, on-demand security controls, real time detection of system intervention and rapid re-constitution of services. While the cloud offers these advantages, until some of the risks are better Understood, many of the significant players will be provoked to hold back. Though cloud computing's aim is to provide better utilization of enriched resources using virtualization techniques and to take up much of the work load from the client, therefore it is loaded with security risks. Because of the critical nature of the applications, it is important that clouds be secure.

There are enormous amount of threats like DDoS attack that can put the adverse effects on the virtualized environment, therefore securing the hypervisor and virtual machines in the cloud environment is important for protecting sensitive data from any intrusions [9].

II. ATTACKS IN CLOUD COMPUTING

Cloud intrusions classification is given as follows:

A. Illegitimate Access:

It is may possible by obtaining the user's password through guessing, stealing, cracking, or the careless influence by the user himself. There may be another possibility of attacking the authentication service and it may result in attack trails left at the service side[1].

B. Misuse:

This would be accomplish through an unauthorized access by a legitimate user. The misutilization of cloud resources are depends on the pre-defined policies or rules or patterns [1].

C. Cloud Attack:

Attacks carry out with the help of tools that focus at vulnerabilities existing in cloud services, protocols and applications. These attacks may be seen in the form of denial-of-service (DOS) attacks and worms[1].

D. Data Security:

Cloud data is deployed in different locations, in various parts of the Earth and hence data security is most challenging task to execute the operation efficiently [1].

III. PRIMAFACIE POLICY TO COPE UP WITH INTRUDERS

Cloud environment has been venerable target from conventional threat or attack such as Distributed Denial of Service (DDoS) attack. A DDoS attack restricts the authentic user from accessing the services [4].

A DDoS attack is the attack on the availability of services of a host server (application server, storage, database Server, or DNS server). DDoS attacks have been a critical challenge to the researchers to make the cloud computing environment fully secure[8]. Hence, for handling the intrusions, its more important to understand the intrusions behaviour. Intruders could be internal or external. External intruders and Internal intruders are most common and dangerous threat for cloud environment. Security policies should state what major steps will be taken to handle intrusion activities. These steps are:

E. Intercept and Avoid:

It is the first step or way to handle intrusions. Prevent the intruder and address the vulnerable activity and don't take any further action [1].

F. Prevent and Scrutinize:

This step aim is to prevent/block the intruder and report the vulnerability. Further action is all about collecting evidence and tries to determine intruder's identity and ultimately investigate about possibility of attack [1].

G. Honey Pot:

Finally allow the attacker to access a part of your network. Meanwhile try to catch the intruder while he explores it. This is a potentially dangerous approach where attackers/intruders may become interested in your site [1].

IV. INTRUSION DETECTION TECHNIQUES

There are two primarily approaches for analyzing events to detect attacks: Anomaly Detection Approach and Misuse Detection Approach. A Misuse detection approach comparing the events or targets with something known attack patterns used by most commercial systems. Anomaly detection, in which the analysis looks for abnormal patterns of activity.

Currently several traditional security tools or systems are provided as a services in the cloud. These systems have been designed and make sure it available to end user to provide the security products for users in a service-based manner. Such model is addressed to as Security-as-a-Service model [10].

A. Anomaly Detection Approach:

Anomaly detectors recognise abnormal unusual behaviour (anomalies) on a host or network. They function on the principle that attacks are different from "normal" (legitimate) activity and can therefore be detected by systems that identify these differences. These Anomaly detectors construct profiles signifying normal behaviour of users, hosts, or network connections.

These profiles are structured from historical data collected over a period of normal operation. After that the detectors gather event data and use a variety of measures to discover when monitored activity deviates from the normal activity. There are many techniques and measure that are used in anomaly detection including; Threshold detection, Statistical measures, Rule-based measures, other measures, including neural networks, genetic algorithms, and immune system models [3].

B. Signature Detection (SD) Approach:

Misuse detectors analyze system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. As the patterns match with known attacks are called signatures. Hence misuse detection is sometimes addressed as "signature-based detection". The most common form of misuse detection used in commercial products specifies each pattern of events corresponding to an attack as a separate signature. Generally Misuse detection techniques, are considered not so effective techniques against the latest attacks that have no matched rules or pattern yet [3].

V. TYPES OF INTRUSION DETECTION SYSTEM

A. Host based IDS:

Host based Intrusion detection Systems (HIDS) are placed at the specific host machine and monitors the inbound and outbound traffic from the host machine. It monitors or inspects host specific network packets. HIDS might detect which program accesses

which resource in the host and discovers that. The drawback of HIDS is that it can't detect the networked attacks; it only looks into the particular system [3].

B. Network based IDS:

Network based Intrusion Detection Systems (NIDS) are placed at the key network points or devices like routers and switches. All the traffic passes through the NIDS. It monitors the network traffic and inspects the packets whether it contains any malicious data. Usually the communication between the hosts is encrypted and NIDS looks unable to detect it that is the drawback of the NIDS. But NIDS is better than HIDS because HIDS protects only one system and using NIDS all the hosts connected to the network can be protected efficiently [3].

In brief, Network intrusion detection systems could able to address outsider threats or attacks and generally have less effectiveness against insider attacks. Whereas Host based intrusion detection systems much more effective to deal with insider attacks but typically must be monitored and managed by cloud users [7].

VI. ATTACKS ON VIRTUAL MACHINES OR HYPERVISORS

A hypervisor or virtual machine manager (VMM) is a piece of computer software, firmware or hardware used to create and runs virtual machines. A computer on which a hypervisor is running one or more virtual machines refer as a host machine. Each of those virtual machines is called a guest machine. Attackers can control the virtual machines by attacking on the hypervisor and consequently can gain access to the host machines. BLUEPILL [5] SubVirt[5] and DKSM[5] are some well-known attacks on virtual layer. Through these attacks, hackers can conciliation the installed-hypervisor to gain control over the host machine. Initially, Firewalls were used to prevent some of the attacks such as EDoS attack, attacks on Virtual Machine etc. Sqalli et al. has given an approach EDoS-Shield for mitigating an EDoS attack in cloud computing. According to the author two significant components of the proposed architecture are virtual firewalls (VF)[5] and verifier cloud nodes (V-Nodes)[5].

The Virtual firewall maintains two lists. The first one is white list to track the authenticated source IP addresses and the second one blacklist to hold unauthenticated source IP addresses. VF monitors the incoming packets from outside the cloud and refered to some services hosted in the cloud and uses these two lists to verify the IP addresses of the incoming packets. Firewall will drop the incoming packets if the IP address of incoming packet will match with the IP addresses stored in the blacklist otherwise this incoming IP address will be added into the white list. Another component a V-Node has the capability to verify legal requests at the application level using graphic Turing tests, such as CAPTCHA.

In this approach the incoming request is captured by the VF and is directed to the V-Node. V-Node presents the requester a graphic Turing Test. Requester solves the test and sends response back to Verifier cloud Node. If the answer to the test is correct, Verifier cloud Node forwards the request to the destined server and adds the source IP address of the request into the white list. Upon receiving the wrong answer, Verifier cloud Node adds this IP into the blacklist and drops the request packets [5].

VII. REVIEW OF PROPOSED SYSTEM

In soft computing, Genetic algorithms are adaptive methods which may be used for optimizing the problem efficiently. The similar phenomenon is employed for handling the intrusions in cloud computing environment. According to the principles of natural selection and survival of the fittest; natural populations are evolved in many generations. Genetic Algorithm is completely evolved along with three basic operators .These operators are [6]:

- Selection
- Crossover
- Mutation

According to author approach in developing an Intrusion detection mechanism for cloud environment protection is quite challenging and motivated for both cloud user and cloud providers. It should include all the basic features of a network based IDS along with the security features for fast and secure access to applications and data.

I just review the author's proposed a three layers based approach to detect the intrusion in cloud environment. The design is depend on Software-as-a Service model for providing the security from threat to the cloud based users.

- Cloud End Users: It represents the users on the cloud network for accessing the cloud facilities [2].
- Hardware Layer: In Author's proposed system need to deploy a hardware layer which is integrated in the cloud network to collect the necessary information. The hardware layer is responsible for securing the entire network. It is incorporated in cloud based on the rules set or threshold to improve the efficiency level and provide the protection flexibility. It further forwards the request to the event service layer through the secure connection layer[2].
- Secure Connection Layer: It is a secure connection path deploy by event service layer to absorb the information from hardware layer otherwise the system behaviour can be corrupt by external intrusion[2].
- Event Service Layer: This layer works as an intermediate layer; it receives the messages from the hardware layer through a secure connection layer checks message and forwards it to the intrusion detection layer[2].

- Intrusion detection System Layer: This layer is the main layer responsible for the intrusion detection. IDS layer consists of sub components to for controlling the intrusion detection. All these sub components have specific functionality to elaborate [2].
- IDS Controller Layer collect the message & it is actually responsible for reading the details and then forwards the items of the interests to the segregator for further segregation of voice data and forwarding it to the Genetic Algorithm Unit.
- Segregate separates the data based on its content and thus in our proposed framework, it segregates the voice data and forwards it to the voice unit.
- Voice section picks the voice records and forwards it to the Genetic Algorithm unit.
- Genetic Algorithm Unit: It is considered as a pattern matching and decision making unit which performs these tasks by using the genetic algorithm technique. It analysis data (voice data) in detail and matches the same with known behaviours which are stored in the existing knowledge base. Fitness Function is the key for checking the match.
- Knowledge Base is the stored knowledge about the prospect cloud service users. It retains the knowledge required for security checks and can be in partial form.
- Notifier is an interface to provide the result reports for analysis to users and the system gathered from the results provided by the genetic algorithm unit.

VIII. CONCLUSIONS AND FUTURE WORK

At the end of discussion we have reached a point where we all well familiar about extreme advantages of adopting the cloud computing technology. But there are various security concerns which must be considered while adopting the cloud computing technology for secure functioning of our systems. This review paper discussed about various intrusions which can violate confidentiality, integrity and availability of Cloud computing environment. One of the promising solution is firewall could not be enough to manage entire cloud security issues at all. Hence the paper emphasise about the handling of intrusions in virtualized environment using one of the powerful technique in soft computing i.e. Genetic methodology. The Cloud computing technology delivers the services such as reducing the infrastructure maintenance cost, scalability for data and applications, availability of data services and pay as you utilized features. There is a need of deeply research to propose an optimize methodology or algorithm which is capable in detecting and preventing intrusions or intruders in cloud computing environment.

REFERENCE

[1] P.Praveen, K.Bhaskar Naik ," A Survey on Cloud Based Intrusion Detection System" International Journal of Software and Web Sciences (IJSWS) 2013.
[2] Umar Hameed, Shahid Naseem, Fahad Ahamd, Tahir Alyas, Wasim-Ahmad Khan ," Intrusion Detection and Prevention in Cloud Computing using Genetic Algorithm" International Journal of Scientific & Engineering Research, Volume 5, Issue 12, December-2014.
[3] Hassen Mohammed Alsafi , Wafaa Mustafa Abduallah and Al-Sakib Khan Pathan," An Integrated Intrusion Handling Model for Cloud Computing Environment ,".
[4] Naresh Kumar and Shalini Sharma, "Study of Intrusion Detection System for DDoS Attacks in Cloud Computing" IEEE, 2013.
[5] Uttam Kumar , Bhavesh N. Gohil ," A Survey on Intrusion Detection Systems for Cloud Computing Environment", International Journal of Computer Applications Volume 109 – No. 1, January 2015.
[6] Vijay.G.R , A. Rama Mohan Reddy , " An Efficient Security Model in Cloud Computing based on Soft computing Techniques", International Journal of Computer Applications Volume 60– No.14, December 2012.
[7] JasonNikolai,YongWang,"Hypervisor-based Cloud Intrusion Detection System"
[8] Anteneh Girma ,Moses Garuba ,Jiang Li, Chunmei Liu, " Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment", 12th International Conference on Information Technology 2015 .
[9] Jaimin K. Khatri , Girish Khilari ," Advancement in Virtualization Based Intrusion Detection System in Cloud Environment", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 5, May 2015.
[10] M.Madhavi," An Approach For Intrusion Detection System In Cloud Computing", International Journal of Computer Science and Information Technologies, Vol. 3 (5) , 5219 – 5222 ,2012.