International Conference on Machine Learning and Computational Intelligence-2017
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 7 | ISSN : 2456-3307

Comparison of Intrusion Detection Techniques in Cloud Computing

Aditya Bakshi[1], Sunanda[2]
[1]Department of Computer Science and Engineering, School of Computer Science and Engineering Shri Mata Vaishno Devi University , Lovely Professional University, Katra, India1, Phagwara, India
[2]Department of Computer Science and Engineering Shri Mata Vaishno Devi University Katra, India

ABSTRACT

This paper has focused on specifying different Intrusion detection techniques in cloud computing. There are different types of attacks that are affecting the cloud are also discussed in this paper. The role of firewall and different intrusion detection techniques in cloud computing for preventing various attacks has also been discussed.

Keywords : Cloud Computing, Firewall, Intrusion Detection System.

I. INTRODUCTION

Cloud computing is the latest computing technology which provides various services on demand and pay per use basis. Fundamental idea behind the evolution of this technology is diversity of computing relative to users. Every user has own needs and expectations from computers and to fulfil them there is a need of various features from computing components i.e. software, hardware and network. It is almost impossible to have every possible computing environment by every user. Especially in case of software development where technology changes every day and clients have varied requirements, software development organizations cannot purchase every development environment for clients. These conditions lead to the evolution of cloud computing where every computing is provided in virtual environment. There are cloud servers created and maintained by computing giants firms which provide numerous services asked by users. Basically cloud services are categorized in three broad categories. First one is Software as a Service (SaaS) which provides various applications especially bounded to software to users. Second one is Infrastructure as a Service (IaaS) which provides various infrastructure environments to users and last one is Platform as a Service (PaaS) which deals with various platforms like OSs, etc [4] [5]. All these services are available to users on pay per use and on demand basis which reduces the cost from earlier stage which was at unaffordable stage to minimal level. Users have to just pay the rent for the time to which they are using services. Apart from this unique feature, cloud computing provides various other features like availability, maintainability, scalability, interoperability, etc. These all facilities cannot be achieved anyhow by standalone users in their local infrastructure due to various unavoidable conditions whereas cloud providers support them due to devoted services.

II. COMMON ATTACKS IN CLOUD

It is crystal clear that cloud computing is the next generation technology which is suitable for all users ranging from any background and having different local computing resources [1]. Although it has attracted researchers and organizations towards its advancements but still it is in its infancy. Moreover there are various security issues due its openness because cloud architecture involves network as Internet and intranets (in some cases). Some of the major intrusions are described as follows

Insider Attack: This is the attack which is performed by insider cloud users. Those users may try to breach the security of cloud by gaining unprivileged access by using their credentials. This is one of the most disastrous threat to cloud because once the internal security architecture will be breached then overall system can be compromised easily.

Flooding attack: This attack is performed by using Zombies which are innocent host and are compromised by attacker to flood cloud environment by various type of request. Those requests may combine ICMP, TCP, UDP, etc. which are sent to just flood the system and in meanwhile various other targets may be compromised to gain access to resources[2].

User to root access: In this attack, those users are compromised which are having root access to the cloud system. Those users can perform administrator level works due to having root level permissions and compromising their credentials may lead to gain of overall system to the attacker [3]. However it is not a single attack based on any paradigm which will be applied and user will be compromised but it involves various other techniques like social engineering as well as eavesdropping, etc. The main motto behind this attack is to gain credentials to reach to the root level of the cloud server which can be further compromised by using the same.

Port Scanning: Port scanning is the technique to scan for all ports of any system. Although it is a manual process to check for each and every port for their status as open or close but there are various automated tools which provide detailed description about any system based on the provided IP address. These tools are sometimes used as a tool to attack cloud environment. Once all open ports which are not being used by any specific service can be used as a back door and automated programs may be deployed to transmit all inform via the same.

Attacks on Virtual Machine (VM) or Hypervisor: Cloud environment is completely based on virtual architecture. It virtualizes both the environments either internal or outer structure. Virtual machine is a dedicated machine based virtually on real environment and may be used to hold other services which may need sophisticated system. The most popular technique for clubbing and splitting VMs is based on hypervisor. There are various known attacks which try to compromise either VMs or target hypervisor to completely choke the system. These attacks always target the layer which works between two layers and compromising any one of the layers would result in the overall compromise of the system. Backdoor or channel attack: Attacker can perform DDoS attack by compromising Zombie system. It may lead to get access to the cloud environment as a backdoor entry which can be used to perform various malicious activities. However in case of malicious activities performed by compromising authorized system is very difficult to detect due to openness and accessibility[6].

Apart from the above discussed attacks there are various other attacks which lead to severe security problems. The common solution to the problem is firewall implementation. However it does not solve

the problems at all which forces the intrusion detection system (IDS) or sometimes intrusion detection and prevention system (IDPS) implementation. First of all we see the features of firewall and various other firewalls which can be implemented and then after various other IDPSs and their comparison in cloud environment [7].

III. FIREWALL

Firewall comprises various set of rules which act as the first line defence mechanism involved in the system. It protects and filters all the incoming and outgoing requests from the system. However, it is completely static in nature working on the pre-defined rules of network. It is unable to protect the system in cases where requests are evasion in nature and here IDPSs play crucial role for the system [8] [9] [10]. Some of the major firewall techniques that are used in cloud environment are Static Packet Filtering Firewall, Stateful Packet Filtering Firewall, Stateful Inspection Firewall and Proxy Firewalls.

Firewalls restrict to some extent in security attacks but not as an overall solution. For sustaining more security in different types of attacks, IDS or IPS can be served as solution that could be incorporate in cloud. However, the different parameters and techniques are required for improving the efficacy of an IDS/IPS in cloud computing. The parameters comprises of different techniques used in IDS and its configuration within the network. Some traditional IDS/IPS techniques such signature based detection, anomaly detection, state protocol analysis etc. can also be incorporated in cloud. The next section covers the common IDS/IPS techniques.

IV. CLOUD IDS TECHNIQUES

A) Signature based detection

This technique incorporates signatures of various known attacks. These signatures are stored in database server of IDS and any incoming or outgoing requests are matched with them. Any matching signature request is discarded immediately from the network or other consequences may be applied like changing the contents, modifying the target, etc. However it is the best technique for known attacks but proves to be very ineffective in case of unknown attacks. Any attack or security breach which is attempted by modifying the content is unable to be detected by this technique. One of the key reason for using signature based detection is because its rules can be easily reconfigured. Reconfiguration of rules is required for updating the signatures of unknown attacks. These signatures are helpful for detecting the network traffic [11].

In cloud, the known attack can be easily detected by using signature based intrusion detection technique. The signature based technique is applied on the front end of cloud for detecting the external intrusion or at back end of cloud for detecting internal intrusions. If signatures are not updated, it cannot be used to detect unknown attacks in cloud.

B) Anomaly detection

Anomaly detection technique tries to detect intrusions that are anomalous to the actual definition. This technique involves various profiles that are used to filter the traffic as genuine or malicious activity. All such profiles are stored in advance as well as dynamically updated based on the uses and traffic pattern. Some of the known products based on this technique are working very well in real life scenarios [12]. Apart from the normal computing, it is also very useful in case of cloud computing. It involves data collection related to the behaviour of legitimate users over training period, and then applies various test which are statistical in nature, are used to observe behaviour and determines genuine user. It is very useful in cases of unknown attacks where definitions

or any specific signatures are unknown in advance. The main idea behind use of this detection technique is to decrease the false alarm rate and work either perfectly either with known or unknown attacks [13].

Anomaly detection techniques detects unknown and known attacks which are segregated at different levels. In cloud, by using anomaly based detection, large number of events (network level or system level) occurs, which makes difficult to monitor or control intrusions.[1].

Capability of soft computing to deal with uncertain and data that is partially true, makes them very useful technique in intrusion detection. There are various techniques from this computing like Fuzzy Logic, Association rule mining, Artificial Neural Network (ANN), Genetic Algorithm (GA), Support Vector Machine (SVM), etc. that can be incorporated to improve the accuracy of detection and efficiency of anomaly detection based IDS and signature based IDS.

C) Artificial Neural Network (ANN) [1] based IDS

ANNs generalises data from incomplete data for intrusion detection and classifies also as normal or intrusive behaviour. Types of ANN used in IDS are as: Back Propagation (BP), Multi-Layer-Feed-Forward (MLFF) nets and Multi-Layer-Perceptron (MLP). Distributed Time Delay Neural Network (DTDNN) has been claimed as the best detection technique in this category till now. It contains capability of classifying and fast conversion rates of data and proves to be a very simple and efficient solution. Its accuracy can be improved by combining various other techniques related to soft computing.

ANN based solutions of IDS proves a better solution over other techniques for network data which are unstructured in nature. Accuracy of intrusion detection involved with these techniques is completely dependent on training profile and layers that are hidden.

D) Fuzzy logic based IDS

FIDS are used for detecting and inspecting various network traffic related to SYN and UDP floods, Ping of Death, E-mail Bomb, FTP/Telnet password guessing and port scanning. Some evolving techniques under Fuzzy Neural Network (FuNN) collaborates both type of learning as supervised and unsupervised learning [1]. EuFNN has better accuracy in intrusion detection than normal ANN techniques and experimental results shown in [1] prove accuracy. Real time intrusions can be also detected in real time environment by involving association rules of Fuzzy System. The experimental results generate two result sets that are mined online from training data. It is very suitable for DoS or DDoS attacks that are implemented on large scale.

E) Association rule based IDS

There are various intrusions that are formed based on known or variants of known attacks. Apriori algorithm for determining the signatures of such attacks are used and they are also capable to determine the variants of such attacks can be determined and detected by frequent itemsets. Data mining technique used in Network based intrusion detection with signature based algorithm generates signatures for misuse detection. However, drawback of the proposed algorithm is involved time consumption which is more than considerable for generating signatures. Scanning reduction algorithm solved this problem which reduces the number of database scans for effectively generating signatures from previously known attacks. However, there are very high false positive rates occur which generate due to unwanted and unknown patterns [1].

F) Support Vector Machine based IDS

SVM is better than other artificial intelligence techniques used with IDS. There are various available experiments which show its efficiency over other techniques. It uses limited sample data to detect

intrusions where accuracy does not get affected due to dimensions of data. False positives rate is also very less than other techniques as experimented in [6]. This is because that various other techniques require large sample dataset whereas it works on a limited sample dataset. Basically SVM works on binary data so for better accuracy, it can be combined with other techniques which can improve its accuracy in detection. SVM is combined with SNORT and some basic rule sets of firewall which allows it to generate a new and effective technique for intrusion detection. The SVM classifier is also used with SNORT to reduce false alarm rate and improve accuracy of IPS. SVM IDS techniques can prove the best techniques for intrusion detection in cloud which can enhance its current feature and extends its security level upto a considerable level.

G) Genetic Algorithm based IDS

GAs use confidence based fitness functions for intrusion detection which classifies network in a very efficient manner. These values can be used and determined for the profile generation as well. These services are very much useful in cases where intrusion behaviors are very dynamic in nature. These techniques can be collaborated with other techniques which are resource intensive and prioritize the overall performance of the system. These techniques use training period and determine the fitness value based on the trained profiles. However, GA can be integrated with other such techniques for better results in cloud technology. This feature is more important than any other techniques involved for intrusion detection. It is also suitable in scenarios wherever there is a need of mutual authentication in cloud among users.

H) Hybrid techniques

Hybrid techniques combine various such technologies together for a better result in sense of intrusion detection. This is such a kind of technology which contains various flavours related to other techniques. NeGPAIM is based on hybrid technique combining two low level components including fuzzy logic for misuse detection and neural networks for anomaly detection, and one high level component which is a central engine analyzing outcome of two low level components. This is an effective model and does not require dynamic update of rules.It is more suitable to be integrated with soft computing techniques which are traditional ones or focused towards intrusion detection. With pros and cons of every technique, this is also not an exception. Some of the limitations under this technique are mainly oriented towards training profiles, period and rules. However, there are various other techniques which can be clubbed with this one to improve the efficiency of the overall system. The lead role in this technique is of algorithm which makes it stand clear form other techniques.

V. CONCLUSION

In this paper, different types of attacks on cloud computing are discussed. This paper has also done a comparison on the different intrusion detection techniques for the securing the cloud from various attacks.

VI. REFERENCES

[1]. Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, A Survey of intrusion detection technques in Cloud, Journal of Network and Computer Applications, Elsevier, 2013, pp. 42-57

[2]. Mohamed, A., Grundy, J., Ibrahim, A. S.: Adaptable, model-driven security engineering for SaaS cloud-based applications. Automated Software Engineering, vol. 21, pp. 187--224. Springer (2013)

[3]. Ye Du, Li, R. Z. M.: Research on a Security Mechanism for Cloud Computing based on Virtualization. Telecommunication Systems, vol. 53, pp. 19—24, Springer (2013)

[4]. Edurado, F. B., Monge. R., Hashizume K.: Building a Security Reference Architecture for Cloud Systems., Requirements Engineering, pp. 1—25. Springer (2015)

[5]. Jin, H., Dong, M., Ota, K., Fan, M., Wang, G.: NetSecCC : A Scalable and Fault Tolerant Architecture for Cloud Computing Security. Peer-to-peer Networking and Applications, pp. 1—15, Springer (2014)

[6]. P, Hu., Sung C. W., Ho, S., Chan, T. H.: Optimal Coding and Allocation for Perfect Secrecy in Multiple Clouds, Information Forensics and Security, vol. 11, pp. 388-399, IEEE (2014)

[7]. Junwon, L., Cho, J., Seo, J., Shon, T., Won, D.: A Novel Approach to Analyzing for Detecting Malicious Network Activity Using a Cloud Computing Testbed, Mobile Networks and Applications, vol. 18, pp. 122-128, Springer (2012)

[8]. Jin, L., Li, Y. K., Chen, X., Lee, P. P. C., Lou, W.: A Hybrid Cloud Approach for Secure Authorized Deduplication, Parallel and Distributed Systems, vol. 26, pp.1206--1216, IEEE Transactions (2014)

[9]. Rahat, M.,Shibli, M. A., Niazi, M. A.: Cloud Identity Management Security Issues and Solutions : A Taxonomy, Complex Adaptive Systems Modeling, vol. 2, pp. 1 – 37, Springer (2014)

[10]. Seungmin, R., Chang, H., Kim, S., Lee, Y. S.: An Efficient Peer-to-peer Distributed Scheduling for Cloud and Grid Computing, Peer-to-peer Networking and Applications, vol. 8, pp. 863 – 871, Springer (2014)

[11]. Li, Q., Han, Q., Sun, L.: Collaborative Recognition of Queuing Behavior on Mobile Phones, Mobile Computing, vol. 15, pp. 60 – 73, IEEE (2014)

[12]. Tak, G. K., Badge N., Manwatkar, P., Rangnathan, A., Tapaswi, S.: Asynchronous Anti Phishing Image Captcha Approach towards Phishing, International Conference on Future Computer and Communication, vol. 3, pp. 694 – 698, IEEE (2010)

[13]. Malhotra, K., Gardner, S., Patz, R.: Implementation of elliptic-curve cryptography on mobile healthcare devices, IEEE (2007)