Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems

SaurabhAdkar,OmkarKelkar,AnujTrivedi,KhushalTrivedi

Computer Department,AISSMS IOIT,saurabhadkar09@gmail.com.

Computer Department,AISSMS IOIT,omkarkelkar18@gmail.com.

Computer Department,AISSMS IOIT,anujtrivedi.at@gmail.com.

Computer Department,AISSMS IOIT,khushalt5@gmail.com.

Abstract-*Cloud security is one of most important issue last few years.Particularly, attackers canexplore vulnerabilities of a cloud system and. A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. In such attack attacker uses one or more agents to attack the actual server service.we proposed a concept of NICE which recognizes different kind of attacks based on different countermeasure. The proposed system builds client-server architecture in which an attacker can perform different types of attacks and nice agent can determine those with relative countermeasures.*
Keywords-*Cloud computing,NetworkSecurity,IntrusionDetection,ZombieDetection,Intrusion Prevention Systems*

INTRODUCTION

Cloud Computing is applications delivered as services across the Internet and the hardware and systems software in the data centers that provide services.The services are referred to as Software as a Service (SaaS).The datacenter hardware and software is known as cloud.

Cloud Computing is one of the emerging field in networking . Cloud networks are less expensive because of lesser software and hardware, does not need large internal storage system ,updating is easy. But with this advantages they are vulnerable for intrusions and malware attacks .for making cloud computing secure we are designing this Network Intrusion Detection and Countermeasure Selection.The illusion of infinite computing resources available on demand, hence eliminating the need for Cloud Computing users to planahead for provisioning.Elimination of an up-front commitment by Cloud users, thereby allowing companies to increase hardware resources only when there is an increase in their needs.The ability to pay for use of the computing resources on a short-term spanas needed and release them as needed, hence rewarding conservation by letting storage go when they are no more useful.

Cloud Computing provides following service capability provided to consumer is to use provider's applications running on cloud infrastructure. The applications are accessible from various client devices through thin client interface like web browser. A consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or even individual application capabilities.Cloud customers can perform port scans on other customers within the internal network.Following Cloud model addresses the security concerns :Map Data Flow-This data flow model maps the data flow between your organization, cloud service,other nodes.It is essential to understand whether & how the data can transmit in or out of the cloud Sketch for each of the models.Knows your risk tolerance!

The exisiting system propose Cloud users can install vulnerable software on their Virtual Machines,which essentially contributes important parts in cloud security. The challenge is to create an effective attack detection and detection system for identifying different attacks. In a cloud system where the infrastructure is shared by nearly millions of users, use of the shared infrastructure benefits attackers to explore vulnerabilities of the cloud.Such attacks are more effective in the cloud environment as cloud users shares computing resources, e.g., being connected via the same switch, sharing with the same data storagesand differentfile systems, even with professional attackers. The similar setup for Virtual Machines in the cloud, e.g., virtualization techniques, Virtual machine OS, installed vulnerable software, networking, etc., attracts attackers to compromise multiple Virtual Machines.

Securtityin Cloud Computing refers to Protecting the datacenters must secure the different cloud resources and hold user's privacy and integrity. Trust networks could be applied to build systems for establishing the trust among

various interactive datacenters. A watermarking technique is suggested to protect data objects and hugely distributed software modules. These techniques safeguard user authentication and fixing the data access-control in a public clouds. The new approach could be less costly than using the traditional encryption and firewalls to secure the clouds.

RELATEDWORK

Saman Taghavi Zargar,James Joshi, and David Tipper[1]:-A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks-we explore the scope of the DDoS flooding attack problem and attempts to combat it. We can make categories of DDoS flooding attacks and then classify existing countermeasuresbased on when they prevent, detect to theDDoS flooding attacks.we highlight the need for a distributed and collaborative defense approach.Our main intention for this work is to stimulate the research community into developing the creative, effective and comprehensive prevention, detection mechanisms that address the DDoS flooding attacks.

Can We Beat DDoS Attacks in Clouds?:-Shui Yu, YonghongTian, Senior Member,SongGuo, and Dapeng Oliver Wu.[2]:- In this paper, we propose dynamic resource allocation strategy to detect DDoS attacks.When a DDoS attack occurs,we employ idle resources of the cloud to clone intrusion prevention servers for the victim in order to filter out intruded packets and gives guarantee of quality of the service for users simultaneously.We establish a mathematical model to approximate the needs of resource investment based on different queueing theory. Through system analysis and real-world experiments, we conclude that we can prevent DDoS attacks in a various cloud environments.

Study of different Intrusion Detection Systems for DdoS Attacks in Cloud systems:-NareshKumar,Shalini Sharma[3]:-DDoS attacks are at the top on the list of cloud attacks from last few years. DDos can cause serious harms, especially to the companies whose business is internet dependant. hence,to decrease the impact of DoS DDoS is one of the important issues. This paper mainly focuses on study of DDoS attacks in cloud computing and the different Intrusion Detection Systems available to work with the issue.

A Survey on different Security Issues and various Threat Models in the Cloud:-Mrs S. Neelima,MrsY.LaxhmiPrasanna,MrsM.Padmavathi[4]:This paper mainly focuses on various Cloud computing security issues to be found within the cloud from both a technical are discussed. The main origin of threats towards data within the cloud is described together with two threat models.The first type of model represents a user-centric view, and the second model is Cloud Service Provider's point of view.

TDFA: Traceback-based Defense against DDoS Flooding Attacks:-VahidAghaeiForoushani, A. NurZincir-Heywood[5]:-This paper mainly focuses on proposing a Trace back-based Defense against DDoS Attacks(TDFA) approach to eliminate this problem. Traceback-based defense consists of following three components: Detection, Traceback, and Traffic Control. In this approach, the aim is to keep the packet filtering as close to the attack source as possible. While doing so,the traffic control component at the victim side focuses to set up a particular limit on the packet forwarding rate to the victim. This type mechanism effectively reduces the rate of forwarding the attack packets to the victim and hence improves the overall throughput of the legitimate traffic.the results based on real world data show that Traceback-based defense is very effective to reduce the attack traffic and to back the quality of service that is QOS for the legitimate traffic.

O. Sheyner, J.Haines, S. Jha and J. M. Wing,"The Automated generation and analysis of attack graphs and attack graph models," Proc.Symp.:- [6]:-This paper mainly focuses on a distributed model concept, the infrastructure of cloud is used by millions of users.Distributed Denial of Service that is Ddos attack has the great potential to make huge impact in cloud computing. In this paper for preventing the vulnerable virtual machine that is VMs from being compromised in the cloud computing,we propose an attack graph model.This model is simple to implement to show all types of attack paths of the host in cloud that is important to understand threats.

S. H. Ahmadinejad, "A hybrid model for correlating alerts of known and unknown attack scenarios"[7]:-The concept of attack graph is used to recognize all types of relationships between the different attack paths. Vulnerability in attack graph means that the alert is mainly towards a real attack. This will not increament the true negative rate. The vulnerability is recognized by the intruder but it is not recognized by vulnerability scanner. In such conditions the alert being real will be considered as false, so false negative rate increases.

ARCHITECTURE DIAGRAM:-

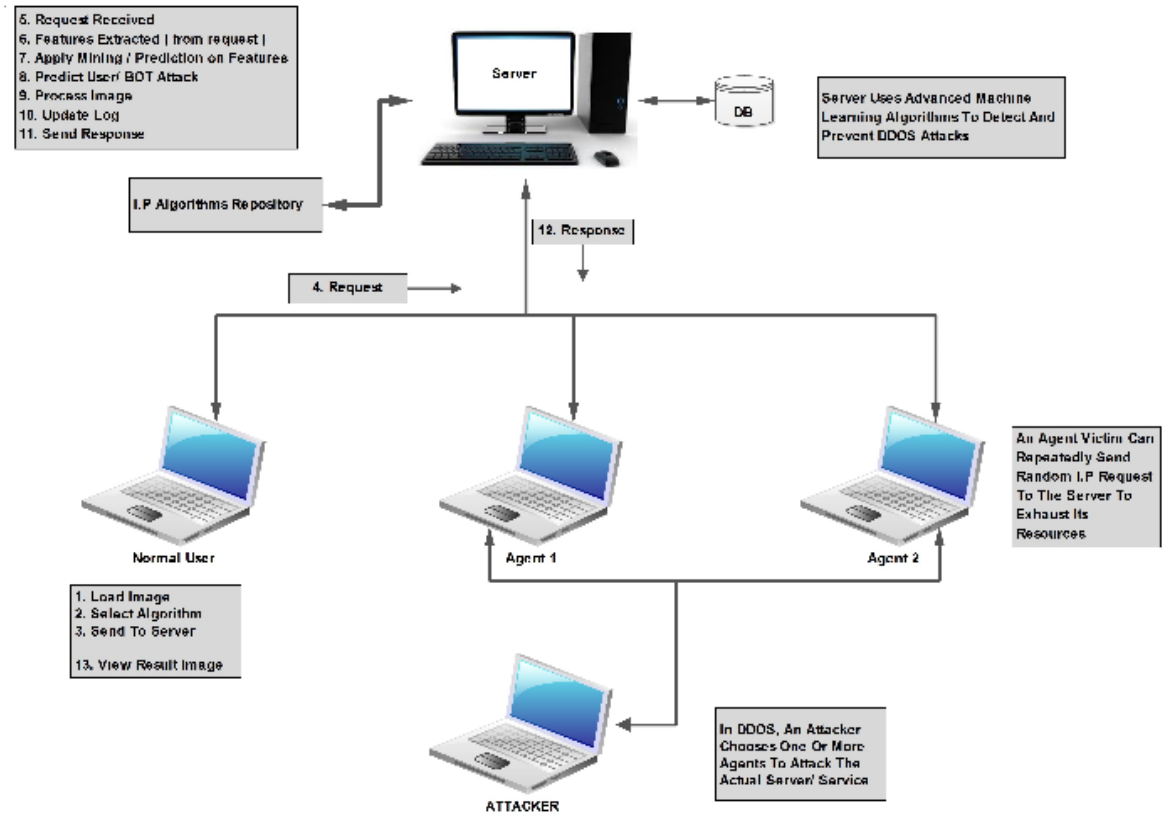

Fig:-Architecture of intrusion detection system

Description

This is basically a client-server Architecture.an attacker sends multiple request to server in order to down it. An attacker can perform different types of attack such as brute force attack,Ddosattack,SQLInjection,Zombie Attack etc. In Ddos ,An attacker chooses one or more agents to attack the actual server services.An agent victim can repeatedly send Random IP requests to the server to exhaust its resources.Server uses advance machine algorithms to detect and prevent attacks.related countermeasures are used to determine particular type of attacks.

No.	Countermeasure	Intrusiveness	Cost
1	Traffic redirection	3	3
2	Traffic isolation	4	2
3	Deep Packet Inspection	3	3
4	Creating filtering rules	1	2
5	MAC address change	2	1
6	IP address change	2	1
7	Block port	4	1
8	Software patch	5	4
9	Quarantine	5	2
10	Network reconfiguration	0	5
11	Network topology change	0	5

Algorithms that we are going to use are K-Means Clustering,Naïve Bayes algorithm.Packet sniffing and sql injection are some important concept as well.K-Means algorithm is basically used in Ddos attacks.

k-means clustering is nothing but an algorithm or you can say a method of vector quantization cluster making, having origin of digital signal processing,which is famous for cluster making and cluster analysis in data mining and data mining applications. *k*-means clustering having goal of making partitions of *n* observations or nodes into *k* number of clusters in which each observation or nodes belongs to the cluster with the nearest mean or minimum difference,providing as a prototype of the cluster.

The problem NP class problem having NP hard type; however, there are various heuristic algorithms that are basically employed and converge quickly to a local optimum solutions.These are basically similar to the expectation-maximization algorithm for combination of Gaussian types of distributions through an iterative refinement approach employed by given all algorithms. Additionally, they both use cluster centroids to classify the data; however, *k*-means clustering sides towards finding clusters of similar nodes or observations,while the expectation-maximization mechanism allows clusters of any kind of shape and can have any number of nodes

The algorithm has a weak relationship to the *k*-nearest neighbor classifier and centroid making, a popular machine learning technique or algorithms for classification that is usually confused with *k*-means because of the word *k* in the name. One can use the 1-nearest neighbor classifying algorithm on the cluster centroids obtained by *k*-means to classify new data or nodes or observations into the existing clusters. This is known as nearest centroid classifier,

Naive Bayes is a simple technique for constructing classifiers: models that assign class labels to problem instances, represented as vectors of feature values, where the class labels are drawn from some finite set. It is not a single algorithm for training such classifiers, but a family of algorithms based on a common principle: all naive Bayes classifiers assume that the value of a particular feature is independent of the value of any other feature, given the class variable. For example, a fruit may be considered to be an apple if it is red, round, and about 10 cm in diameter. A naive Bayes classifier considers each of these features to contribute independently to the probability that this fruit is an apple, regardless of any possible correlations between the color, roundness and diameter features.

Abstractly, naive Bayes is a conditional probability model: given a problem instance to be classified, represented by a vector,

$$\mathbf{x} = (x_1, \ldots, x_n)$$

representing some *n* features (independent variables), it assigns to this instance probabilities

$$p(C_k|x_1, \ldots, x_n)$$

for each of *K* possible outcomes or *classes*.[7]The problem with the above formulation is that if the number of features *n* is large or if a feature can take on a large number of values, then basing such a model on probability tables

is infeasible. We therefore reformulate the model to make it more tractable. Using Bayes' theorem, the conditional probability can be decomposed as

$$p(C_k|\mathbf{x}) = \frac{p(C_k)\ p(\mathbf{x}|C_k)}{p(\mathbf{x})}.$$

REFERENCES

[1]M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski,G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,"A view of cloud computing," ACM Commun, Apr. 2010.

[2]B. Joshi, A. Vijayan, and B. Joshi, "Securing cloud computing environment against DDoS attacks," IEEE Int'l Conf. Computer Communication and Informatics (ICCCI '12), Jan.2012.

[3]H. Takabi, J. B. Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Security & Privacy, pp Dec. 2010.

[4]"Open vSwitch project," http://openvswitch.org, May 2012.

[5]Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, andJ. Barker, "Detecting spam zombies by monitoring outgoing messages,"IEEE Trans. Dependable and Secure Computing 198–210, Apr. 2012.

[6]G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, "BotHunter:detecting malware infection through IDS-driven dialog correlation," *Proc. of 16th USENIX Security Symp. (SS '07)* Aug. 2007.

[8] G. Gu, J. Zhang, and W. Lee, "BotSniffer: detecting botnet command and control channels in network traffic," *Proc. of 15th Ann.Network and Distributed Sytem Security Symp. (NDSS '08)*, Feb. 2008.

[9] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing,"Automated generation and analysis of attack graphs," *Proc. IEEESymp. on Security and Privacy*, 2002.

[10] "NuSMV: A new symbolic model checker," http://afrodite.itc.it:1024/nusmv. Aug. 2012.

[11] S. H. Ahmadinejad, S. Jalili, and M. Abadi, "A hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs," *Computer Networks*,2221–2240, Jun. 2011.

[12] X. Ou, S. Govindavajhala, and A. W. Appel, "MulVAL: a logicbasednetwork security analyzer," *Proc. of 14th USENIX Security Symp.*, 113–128. 2005.

[13] R. Sadoddin and A. Ghorbani, "Alert correlation survey: framework and techniques," *Proc. ACM Int'l Conf. on Privacy, Securityand Trust: Bridge the Gap Between PST Technologies and BusinessServices (PST '06)*. 2006.

[14] L. Wang, A. Liu, and S. Jajodia, "Using attack graphs for correlating,hypothesizing, and predicting intrusion alerts," *ComputerCommunications*, Sep. 2006.

SUMMARY AND CONCLUSION

We propose NICE that is Network Intrusion detection and Countermeasure selection in virtual network systems to establish intrusion detection system. For effective attack detection, NICE implemets attack graph model and analytical procedures into the process of intrusion detection.We must note that the design of NICE does not having

any intend to improve any of the currently available intrusion detection algorithms; but,NICE employs a effective reconfigurable virtual networking and cloud computing approach to detect and counter the attempts to compromise VMs, thus preventing zombie VMs.

The intent of this project was to make cloud networking providing software as a service secure and safer for users. We are going to implement a Network Intrusion Detection and Countermeasure Selection mechanism for a Cloud Network. Cloud computing is emerging in networking field so we propose this mechanism in to make it quite efficient and effective computing .To increase the performance of system security is important feature. So we design a NICE mechanism to achieve all these features and charectiristics.

In this paper, we presented NICE, which is proposed to detect and prevent different collaborative attacks in the cloud computing and virtual networking systems.NICE makes use of the attack graph model for attack detection and prediction. The proposed solution finds out how to use the programmability of different software switches based types solutions to improve the detection and prevention accuracy and defeat different victim exploitation phases of collaborative attacks. The system performance evaluation demonstrates the feasibility of NICE and shows that the proposed solution can significantly decrease the risk of the cloud system from being exploited and abused by internal and external attackers and intruders .NICE only finds out the network IDS approach to eliminate zombie explorative attacks. For improving the detection accuracy, host-based IDS solutions are must be incorporated and to cover the every part of IDS in the cloud computing system. This should be investigated in the upcomting work.Additionally, as given in the paper, we will find out the scalability and reliability and flexibility of the proposed NICE solution by finding out the decentralized network control and attack analysis model based on current study.