International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-3, March 2015

Secure Conserve Data Split To Avoid Network Intrusion Detection

R.Sasikala, J.Revathi

Abstract— **Cloud security is one of most keyconcerns that have involved a lot of research and development power in past years. Predominantly, attackers can discoversusceptibilities of a cloud system and conciliation virtual machines to organizeauxiliary large-scale Distributed Denial-of-Service (DDoS). DDoS attacks typicallyinclude early stage actions such as multistep exploitation, low-frequency susceptibility scanning, and compromising identified vulnerable virtual machines as zombies, and finally DDoS attacks through the conceded zombies. However, it is also well known that model checkers suffer from scalability problems, and there is good cause to doubt whether a model checker can gripopenly a genuine set of deeds for even a modest sized network. Cloud Computing is a flexible, proven delivery platform and cost-effective for providing business or consumer IT services over the Internet. Cloud Computing influences many technologies It also receives their security problems, which we discuss here, recognizing the main susceptibilities in this kind of systems and the most important intimidations found in the literature related to Cloud Computing and its environment as well as to recognize and relate liabilities and threats with possible solutions. To prevent vulnerable virtual machines from being negotiated in the cloud, we suggest a multi-phase distributed vulnerability detection, countermeasure selection mechanism and measurement called NICE, which is assembled on attack graph-based diagnostic models and reconfigurable virtual network-based countermeasures. Furthermore, as indicated in the paper, we will explore the scalability of the proposed NICE solution by inspecting the decentralized network control and attack examination model.**

***Index Terms*— Distributed Denial of Service Attack, Network Intrusion System.**

I. INTRODUCTION

The applications used are classically delivered via the Internet through a Web browser. Yet, defects in web claims may create susceptibilities for the SaaS applications. Invaders have been using the web to cooperation user's computers and perform malicious events such as steal subtle data. Security challenges in SaaS applications are not altered from any web application technology neverthelessoutdated security solutions do not efficientlydefend it from attacks, so new methods are necessary. The Open Web Application Security Project (OWASP) has identified the ten most perilous web applications security intimidations. There are more security problems, but it is a good start for safeguarding web applications.

The Virtual Machine Monitor (VMM) or hypervisor is accountable for virtual machines isolation; consequently, if the VMM is cooperated, its virtual machines may hypothetically be conceded as well. The VMM is a software that controls and observes its virtual machines, so as any traditional software it requires security defects. Possession the VMM as simple and small as potential reduces the risk of security liabilities, as it will be easier to find and fix any susceptibility. Furthermore, virtualization introduces the capability to wander virtual machines between physical servers for fault tolerance, maintenance or load balancing. This valuable feature can also increase security issues. An attacker can give and take the relocation module in the VMM and transmissionof a victim virtual machine to a malicious server. Also, it is clear that VM migration depict the content of the VM to the network, which can cooperate its data integrity and privacy. A malicious virtual machine can be migrated to another host (with another VMM) negotiating it. Countermeasures for T010: sniffing/spoofing virtual networks Virtual network security a virtual network framework that safeguards the communication between virtual machines. This framework is based on Xen which bids two configuration modes for virtualnetworks: "bridged" and "routed". The virtual network model is comprises of three layers: routing layers, firewall, and shared networks, which can avoid VMs from sniffing and spoofing. An assessment of this approach was not accomplished when this publication was published. Besides, web services are the largest implementation technology in cloud environments. Nevertheless, web services also lead to several challenges that need to be addressed. Security web services idealsdefine how to protect communication among applications through integrity, authentication,confidentiality and authorization.

Manuscript received March 24, 2015.

R.Sasikala, PG Student STET Women's college, mannargudi

J.Revathi, Asst.Professor of CS department, STET Women's college, mannargudi

II. LITERATURE REVIEW

A.M.Lonea, D.E. Popescu, H. Tianfield [01] focus on detection and analyzation of Distributed Denial of Service (DDoS) attacks in cloud computing environments we have proposed a solution using Dempster-Shafer Theory (DST) operations in 3-valued logic and the Fault-Tree Analysis (FTA) for each VM-based Intrusion Detection System (IDS). At the same time, the usability requirement has been accomplished, because the work of cloud administrators will be alleviated by using the Dempster rule of evidence combination whereas the number of alerts will decrease and the conflict generated by the combination of information provided by multiple sensors is entirely eliminated.

I.Mettildha Mary , P.V.Kavitha , Priyadharshini M , Vigneshwer S Ramana [02] focus on cloud computing model has the ability to scale computer resources on demand, and give users a number of advantages to progress their conventional cluster system. One of the most serious threats to cloud computing security itself comes from Distributed Denial of Service attacks. These types of attacks are simple and easy to implement by the attacker, but to security experts

they are twice as difficult to stop. So, a solution model is offered to Trace Back through proposed Cloud Trace Back (CTB) to find the source of real attacks, and introduce the use of a back propagation neutral network, called Cloud Protector,Economic Denial of Sustainability attacks are more relatively connected to the economical resources coupled to the cloud environment those are should be secured. This was trained to detect and filter such attack traffic.

Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker [03] focus on effective pam zombie detection system named SPOT by monitoring outgoing messages in a network. SPOT was designed based on a simple and powerful statistical tool named Sequential Probability Ratio Test to detect the compromised machines that are involved in the spamming activities. SPOT has bounded false positive and false negative error rates. It also minimizes the number of required observations to detect a spam zombie.

G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee [04] focus on design and implementation of BotHunter, a perimeter monitoring system for real-time detection of Internet malware infections. The corner-stone of the BotHunter system is a three-sensor dialog correlation engine that performs alert consolidation and evidence trail gathering for investigation of putative infections. We evaluate the system's detection capabilities in an in situ virtual network and a live honeynet demonstrating that the system is capable of accurately flagging both well-studied and emergent bots. We also validate low false positive rates by running the system live in two operational production networks.

G. Gu, J. Zhang, and W. Lee [05] focus on BotSniffer successfully detected all botnets and generated very few false positives. In addition, its correlation engine generated accurate and concise report rather than producing alerts of malicious events (e.g., scanning, spamming) as a traditional IDS does. For instance, in trace All-4, the monitor engine produced over 100 activity events, none of which is the indication of actual botnets (e.g., they are false positives), while the correlation engine did not generate a false positive. In another case, e.g.,in V-Spybot, there were over 800 scanning activity events produced by the monitor engine, and the correlation engine only generated one botnet report (true positive), which was a great reduction of work for administrators.

N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, and S. Shenker [06] focus on etworks are managed through low-level configuration of individual components. Moreover, these configurations often depend on the underlying network; for example, blocking a user's access with an ACL entry requires knowing the user's current IP address. More complicated tasks require more extensive network knowledge; forcing guest users port 80 traffic to traverse an HTTP proxy requires knowing the current network topology and the location of each guest. In this way, an enterprise network resembles a computer without an operating system, with network-dependent component configuration playing the role of hardware-dependent machine language programming

III. NETWORK INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) is a method or software application that displays network or system events for malicious activities or policy abuses and createsinformation to a management station. IDS come in a variability of "flavors" and approach the goal of perceivingdistrustful traffic in diverse ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may challenge to stop an intrusion effort but this is neither necessary nor predictable of a monitoring scheme. Intrusion detection and prevention systems (IDPS) are primarily intensive on recognizing possible occurrences, logging facts about them, and reporting attempts. In addition, administrations use IDPSes for other resolutions, such as identifying problems with security policies, verifying existing threats and daunting individuals from unconventional security strategies. IDPS have become a necessary addition to the security infrastructure of approximately every organization.

IV. WORKING

Cloud user

Cloud users frequentlysegment computing resources, e.g.,being associated through the same switch, distribution with the same data storage and file systems. Cloud consumers may install vulnerable applications on their fundamental machines.

Cloud service provider

The cloud service provider is answerable for preserving an agreed-on level of service and necessities resources accordingly. A CSP, who has noteworthyproperties and expertise in building and managing distributed cloud storage servers, preserves and functions live Cloud Computing systems,. It is the central entity of cloud. A cloud provider activity is helpful for using and allottingunusual resources within the limit of cloud environment so as to meet the needs of the cloud application. It needs the type and amount of properties needed by each application in order to finish a user job. The order and time of allocation of capitals are also an input for an optimal reserve allocation.

Network intrusion detection and counter measure selection-agent (NICE-A)

The input is the attack graph G, and a pool of countermeasures CM. The algorithm proceed by selecting the node vAlert that resembles to the alert generated by a NICE-A. The countermeasure which when functional on a node gives the least value of ROI. It is regarded as the optimal countermeasure.

Attack analyzer

The major purposes of NICE system are accomplished by attack analyzer, which consist ofprocesses such as attack graph construction, alert correlation, update and countermeasure selection. NICE attack graph is created based on the following data:

- Cloud system data is composed from the node controller and VM's Virtual
- Interface (VIF) information is used.
- Virtual network topology and configuration data is composed from the network controller, every VM's IP address, port information,MAC address and traffic flow information.

Network controller

The network controller is a key element to support the programmable networking competence to recognize the virtual network reconfiguration feature based on Open- Flow

protocol. The network controller is answerable for collecting network information of current OpenFlow network and offers input to the attack analyzer to create attack graphs.

Vm profiling

Virtual machines in the cloud can be outlined to get exact information about their state, open ports,services running etc. VM profiles are preserved in a database and contain inclusive information about susceptibilities, alert and traffic.

Performance evaluation

We evaluate system enactment to offer guidance on how much traffic NICE can control for one cloud server and use the evaluation metric to gage up to a large cloud system. In a real cloud system,our evaluation is directed in two directions: the system computing and security performance. And network reconfiguration overhead occurs due to introduced security mechanism.

V. ARCHITECTURE DIAGRAM

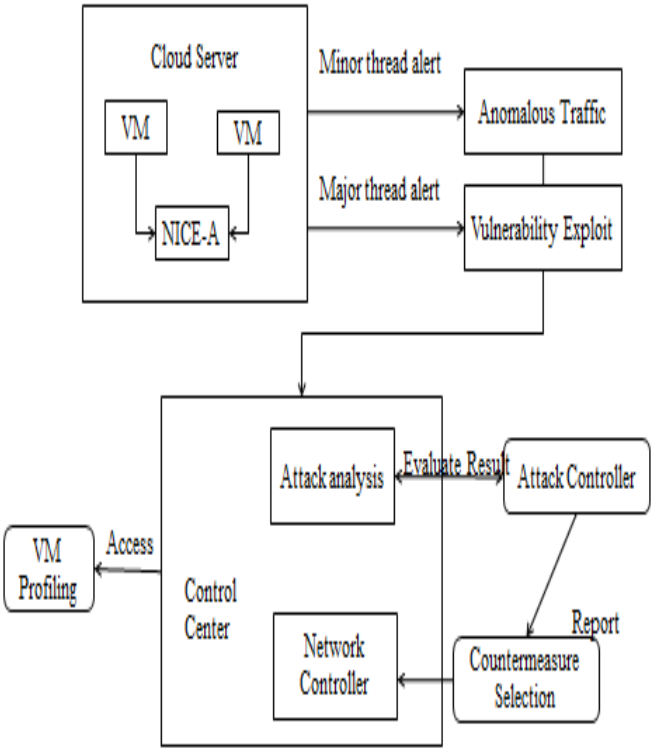

Fig 1.1 Intrusion Control System

VI. CONCLUSION

Cloud Computing is a moderately new concept that offers a good number of welfares for its users; however, it also advances some security difficulties which may slow down its use. Accepting what vulnerabilities exist in Cloud Computing will help administrations to make the shift towards the Cloud. Since Cloud Computing controls many technologies, it also gets their security issues. Traditional web applications, virtualization and services running have been observed over, but certain of the solutions presented are immature or inexistent. We have offered security issues for cloud models: IaaS, IaaS and PaaS which differliable on the model. As defined in this paper, storage and networks are the biggest security problems in Cloud Computing. Virtualization which permits multiple users to segment a physical server is one of the major issues for cloud users. Also, additional challenge is that there are diverse types of virtualization technologies, and each type may approach security devices in dissimilar ways. Virtual networks are also objective for some attacks predominantly when collaborating with remote virtual machines.

REFERENCES:

[1] A.M. Lonea, D.E. Popescu, H. Tianfield," Detecting DDoS Attacks in Cloud Computing Environment", ISSN 1841-9836, 8(1):70-78, February, 2013.

[2]I.Mettildha Mary , P.V.Kavitha , Priyadharshini M , Vigneshwer S Ramana,"Secure Cloud Computing Environment against DDOS and EDOS Attacks",International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014.

[3] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J.Barker, "Detecting Spam Zombies by Monitoring Outgoing Messages," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 198-210, Apr. 2012

[4] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, "BotHunter: Detecting Malware Infection through IDS-driven Dialog Correlation," Proc. 16th USENIX Security Symp. (SS '07), pp. 12:1-12:16, Aug. 2007.

[5] G. Gu, J. Zhang, and W. Lee, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic," Proc. 15th Ann. Network and Distributed Sytem Security Symp. (NDSS '08), Feb.2008.

[6] N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, and S. Shenker, "NOX: Towards an Operating System for Networks," SIGCOMM Computer Comm. Rev., vol. 38, no. 3, pp. 105-110, July 2008.

CORRESPONDING AUTHOR

R.Sasikala, PG Student STET Women's college, mannargudi, Tamilnadu

J.Revathi, Asst.Professor of CS department, STET Women's college, mannargudi, Tamilnadu