International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Comprehensive Comparative Study on Intrusion Detection System in Cloud Computing

Gayatri P[1], PriyankaRao N[2], Nishanth N[3], AbishekRaghav[4], Mrs.Vani K.A[5]
[1,2,3,4]*Undergraduate Students,* [5]*Assistant professor*
Department Information Science of Engineering
Dayananda Sagar College of Engineering, Bangalore, Karnataka

Abstract-Cloud computing involves deploying groups of remote servers and software networks that allow different kinds of data sources be uploaded for real time processing to generate computing results without the need to store processed data on the cloud. The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.Security is one of the concerns about cloud computing that is delaying its adoption. One of the biggest security concerns about is that when you move your information over the cloud you will lose control of it. The cloud gives you the access data, but you have no way of ensuring no one else has access the data. Intruders are the network security attackers intend to breach cloud security. In spite of security issues cloud computing has become very essential needs of the industry. One of the security mechanisms to prevent this issue is Intrusion Detection Systems (IDS). In this paper our focus is to design an Intrusion Detection System (IDS) to defend against the cloud intruders.
Keywords: Intrusion Detection System, Security, DDoS

I. INTRODUCTION

Cloud computing is an emerging technology that allows customers to obtain computing services and resources such as networks, service, storage and applications. Cloud computing technology has been facing some security issues. Cloud computing operational models, enabling technologies and its distributed nature, clouds are easy targets for intruders looking for possible vulnerabilities to exploit. However, with the extensive use of cloud computing, security issues came out on a growing scale. It is necessary to solve the security issues to promote the wider applications of cloud computing. To provide secure and reliable services in cloud computing environment is an important issue. One of the techniques to detect the above security issues is IDS. Therefore, an Intrusion detection system (IDS) is a security system that monitors computer systems and network traffic and analyses that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization. Therefore, cloud computing system needs to contain some Intrusion detection Systems (IDSs)for protecting each virtual machine against threats. If the IDS provide stronger security services using more rules or patterns, then it needs much more computational resources in proportion to the strength of security. Another problem in cloud computing is that, it is hard to analyse amount huge of logs by system administrators.

Intrusion detection provides the following:
Monitoring and analysis of user and system activity
Auditing of system configurations and vulnerabilities
Assessing the integrity of critical system and data files
Statistical analysis of activity patterns based on the matching to known attacks
Abnormal activity analysis
Operating system audit

II. ALLIED EXERTION

A.Dinesha H A et.al [6] describes the emerging usage of cloud computing services, the misuse of possible vulnerabilities grows at the same speed. The distributed nature, on demand services, wide usage of the cloud computing makes it an attractive target for potential intruders. Intruders are the network security attackers intend to breach cloud security. Despite security issues delaying cloud adoption, cloud computing has already become an inescapable needs and ready industry solutions. Thus, security mechanisms to ensure its secure adoption are in demand. One security mechanism is intrusion detection and prevention systems (IDPS). IDPS have been used widely to detect malicious behaviors in network communication and hosts. Here, we focus on IDPS to defend against the cloud intruders. They propose a technique called cloud service usage profile based IDPS technique. This technique is to detect and prevent intruders in cloud service intrusion based on the cloud service usage profile. In turn, this usage profile helps to detect unusual usage and prevent intrusion.

B.Oscar Rodas, Jose Alvarez et.al [12] describes the Intrusion Detection System (IDS) industry has worked on bringing a

solution to anomaly based attacks on computer networks. The main concerns related to the IDS implementations have been: the low detection rate of anomaly-based attacks that provokes low usability and high rate of false positives that cause low acceptability. Researchers in the field of IT have proposed different approaches using numerous techniques to improve these rates. In the paper they bring an approach based on the problematic faced by networks when anomaly-based attacks emerge. Their approach proposes a novel framework based on analyzing real-time information and classifying traffic in a binary way, legitimate or an intrusion.

C.Bansidhar Joshi et.al [9] describes that the cloud computing is becoming one of the next IT industry buzz word. However, as cloud computing is still in its infancy, current adoption is associated with numerous challenges like security, performance, availability, etc. In cloud computing where infrastructure is shared by potentially millions of users, Distributed Denial of Service (DDoS) attacks have the potential tohave much greater impact than against single tenanted architectures. In the paper the efficiency of a cloud trace back model in dealing with DDoS attacks using back propagation neural network and finds that the model is useful in tackling Distributed Denial of Service attacks.

D.GurudattKulkarni et.al [2] describes deploying cloud computing in an enterprise infrastructure brings significant security concerns. Successful implementation of cloud computing in an enterprise requires proper planning and understanding of emerging risks, threats, vulnerabilities, and possible countermeasures. They believe enterprise should analyze the company/organization security risks, threats, and available countermeasures before adopting this technology. In a cloud computing environment, the entire data reside over a set of networked resources, enabling the data to be accessed through virtual machines. Since these data centres may lie in any corner of the world beyond the reach and control of users, there are multifarious security and privacy challenges that need to be understood and taken care of. Also, one can never deny the possibility of a server breakdown that has been witnessed, rather quite often in the recent times. There are various issues that need to be dealt with respect to security and privacy in a cloud computing scenario. This extensive survey paper aims to elaborate and analyze the numerous unresolved issues threatening the Cloud computing adoption and diffusion affecting the various stake-holders linked to it.

E.AkhilBehl [4] describes cloud computing has changed the whole picture that distributed computing used to present e.g. Grid computing, server client computing. Cloud has given a new meaning to distributed, and off-premises computing. Although, Cloud offers great benefits, it also introduces a myriad of security threats to the information and data which is now being ported from on-premises to off-premises. Where cloud computing can help organizations accomplish more by paying less (in the longer run) and breaking the physical boundaries between IT infrastructure and its users, due to openness of accessible information and data relying on trust between cloud provider and customer, heightened security threats must be overcome in order to benefit fully from this new computing exemplar. This paper explores the security issues related to the cloud. This paper also discusses the existing security approaches to secure the cloud infrastructure and applications and their drawbacks. Finally, we explore some key research challenges of implementing new cloud-aware security solutions that can provide the likes of pre-emptive protection for complex and ever dynamic Cloud infrastructure, followed by conclusion where we try to entail the whole research and try to formulate a security strategy which will enable the Cloud providers and customers alike to fight against ever emerging security threats.

III. TYPES OF INTRUSION ATTACKS

Thedifferent types of intrusion attacks and standard solutions arediscussed below:

A. Insider Attack

In authorised cloud user or insiders may commit frauds and disclose information to others. The solution for this attack is Signature based intrusion detection.

B. Flooding Attack

The attacker tries to flood victim by sending huge number of packets from innocent host in network. It leads to fake usage of cloud virtual machines. The solution for this attack is that either signature based intrusion detection or anomaly based intrusion detection techniques can be used.

C. User To Root Attacks

The attacker gets an access to legitimate user's account by sniffing password. In case of cloud, attacker acquires access to valid user's instance which enables him/her for gaining root level access to virtual machines or host. The solution for this type of attack is that initially anomaly based intrusion detection techniques can be used. Later signature based intrusion detection can be used. But it blocks the genuine user.

D. Port Scanning Attack

The attackers can find open ports and attack on services running on these ports. Network related details such as IP address, MAC address, router, gateway filtering, firewall rules etc. can be known through this attack. In cloud scenario, attacker can attack offered services. The solution for this attack can be solved using an anomaly based intrusion techniques and later signature based intrusion detection can be used. But it blocks genuine ports.

E. Attacks On Virtual Machine

By compromising the lower level hypervisor, attacker can gain control over installed virtual machines. Through these attacks, hackers can be able to compromise installed-hypervisor to gain control over the host. This attack can be resolved using anomaly based intrusion detection technique.

F. Backdoor Channel Attacks

It is a passive attack which allows hackers to gain remote access to infected node in order to compromise user confidentiality. In cloud environment, attacker can get access and control cloud users resources through backdoor channel and make virtual machine as zombie to initiate DOS/DDoS attack. The solution for this type of attack is we can either use signature based intrusion detection and anomaly based intrusion detection techniques.

IV. EXISTING INTRUSION DETECTION SYSTEM (IDS)

The different types of IDS are Signature-based IDS, Anomaly Detection IDS, Host-based IDS, Network-based IDS and Distributed IDS.

A. Signature Based IDS

It identifies intrusion by matching patterns with preconfigured knowledge base. It has high detection accuracy for previously known attacks and low computational cost.The limitations of this technique are only the existing signatures of attacks will be detected and constant update is required to
detect the signatures of new attacks. For suspicious and unknown attacks there will high false alarm rate.

B. Anomaly Detection IDS

It uses statistical on collected behaviour to identify intrusion and can lower the false alarm rate for unknown attacks.The limitations of technique are it requires more time to detect the attacks in the network.

C. Host-Based IDS (HIDS)

It identifies intrusions by monitoring hosts file systems, system calls or network events.The limitations of this technique are
it can monitor attacks only on the host where it is deployed. This IDS is not suited for network scans and any surveillance that targets on the entire network.

D. Network Based IDS (NIDS)

It identifies intrusions by monitoring network traffic; it should be placed only on under lying network and can monitor multiple systems at a time.The limitation of this technique areit fails to recognize the attack that is launched during the period of high traffic and it cannot identify encrypted information. NIDS cannot detect whether an attack is successful or not.

E. Distributed IDS (DIDS)

It uses characteristics of both HIDS and NIDS and thus inherits benefit from both of them.The limitations of this technique are, if the central server is overloaded it is difficult to operate in centralised distributed intrusion detection system. The communicational and estimated cost is high.

V. PROPOSED METHOD

A DDoS(Distributed Denial of Service) attack prevents the legitimate user from accessing the service. The defence techniques of DDoS are divided mainly into three aspects: detection, identification andfiltration. One of the most effective mechanisms for detectionand prevention of DDoS is the use of Intrusion DetectionSystem.To improve the detection accuracy, host-based Intrusion Detection System (HIDS) solutions are needed to be incorporated and to cover the whole spectrum of IDS in the cloud system.In this proposed system an external agent is used to improve theattack detection probability and improve the resiliencyto VM exploitation attack without interruptingexisting normal cloud services.The external agent is a software agent, implemented in each cloud server connected to the control center through a dedicated and isolated secure channel, which is separated from

the normal data packets using VLAN approaches.

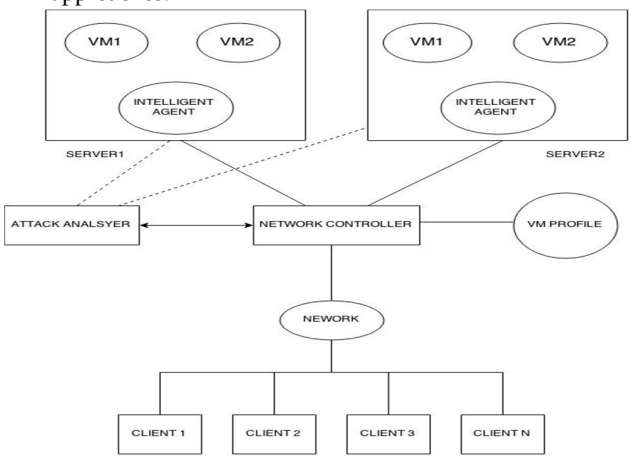

Figure 1: System Architecture

The above shown figure shows how the external agent works. Here we use intelligent agent as an external agent who is used to detect an attack and it informs to attack analyser which accepts the message from the external agent and checks whether the user who is creating the attack is present in the database or else if it is a new attacker it enters into the scenario based analysis. In scenario based analysis we monitor the behaviour of the user and decide whether to block him or not and informs to the network controller whether to block the user or not. We make use of this external agent to overcome the limitation of IDS.This will help us in controlling the traffic in the VLANs by blocking the intruder. This is done by external agent which monitors the user behaviour and the attack analyser will decide whether to block the user or give the access.

VI. CONCLUSION AND FUTURE WORK

In cloud computing environment there are many benefits and more customer usage demand. It gives cost benefits by providing ready infrastructure and effective resource management. However, security is the main issue which needs to be resolved on priority basis. Intrusion Detection System are available in literature. Specific to cloud security and intrusion, effective technique requires on high priority basis. In this paper we have discussed about IDS which is necessary in any environment. Than Intrusion detection systems the external agent that we are proposing has many applications which reports about the intruder. The future work for this paper can be enhanced by making the attack analyser incorporated in the network controller so that cost andtime consuming can also be reduced and performance can also be increased.

REFERENCES

[1] Hisham A. Kholidy, FabrizioBaiardi CIDS: A framework for Intrusion Detection in Cloud Systems, 2012 Ninth International Conference on Information Technology- New Generations, 978-0-7695-4654-4/12 $26.00 © 2012,pp 379-385.
[2]GurudattKulkarni, Nikita Chavan,RuchiraChandorkar ,RajnikantPalwe, Cloud Security Challenges, 2012 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA).
[3] T. Udaya, V. Vijay, and A. Naveen, “Intrusion detection techniques for infrastructure as a service cloud,” in Proceedings of the 9th IEEE International Conference on Dependable, Autonomic and Secure Computing, IEEE Computer Society, pp. 744–751, Sydney, Australia, 2011.
[4] AkhilBhel, “Emerging Security Challenges in Cloud Computing”, Information and Communication Technologies, 2011 World Congress on, Mumbai, 11th - 14th Dec 2011, pp 217 - 222, Print ISBN: 978-1-4673-0127-5, DOI: 10.1109/WICT.2011.6141247.
[5] Modi, C., Patel, D., Patel, H., Borisaniya, B., Patel, A. &Rajarajan (2012). A survey of intrusion detection techniques in Cloud. Journal of Network and Computer Applications, doi: 10.1016/j.jnca.2012.05.003
[6]Cloud Services Usage Profile Based Intruder Detection and Prevention System: Intrusion Meter Dinesha H A and Vinod Kumar Agrawal,PES Institute of Technology, Visvesvaraya Technological Univeristy, Belgaum, India; sridini@gmail.com; 2vk.agarwal@pes.edu
[7]Daniel E O’Leary,”Intrusion Detection System” https:// msbfile03. usc.edu/digital measures/doleary/ intellcont/intrusion detection and continuous auditing_1.pdf
[8] C. B. Westphall and F. R. Lamin. SLA Perspective in Security Management for Cloud Computing. In Proc. of the Int. Conf. on Networking and Services (ICNS), 2010. Pp. 212-217.
[9]Bansidhar Joshi, A. SanthanaVijayan, Bineet Kumar Joshi,”Securing cloud computing environment against ddosattacks”International Conference on Communication, Volume 5.
[10] Karen Scarfone and Peter Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS)”, National Institute of Standards and Technology(NIST), Special Publication 800-94, Feb. 2007.
[11] Gupta, S. Horrow, and A. Sardana, “IDS based defense for cloud based mobile infrastructure as a service,” in Proceedings of the 8th IEEE World Congress on Services (SERVICES), pp. 199–202, Honalulu, Hawaii, USA, 2012.

[12]A novel Classication-based Hybrid IDS Oscar Rodas1, Jose Alvarez1, Gerardo Morales1, Stephane Maag2 Research Lab in Information & Communication Technologies/Universidad Galileo1 Institu Mines-Telecom/Telecom SudParis2, 2014.
[13] Data set, 1999 DARPA Intrusion Detection Evaluation Data Set. http://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/data/1999data.html,1999.
[14] M Ali Ayd_n, AHalimZaim, and K G okhanCeylan. A hybrid intrusion detection system designfor computer network security. Computers& Electrical Engineering, 35(3):517-526, 2009.
[15] Karan Bajaj and AmitArora. Improving the intrusion detection using discriminative machinelearning approach and improve the time complexityby data mining feature selection methods.International Journal of Computer Applications, 76(1):5-11, 2013.
[16] Chia-Mei Chen, Ya-Lin Chen, and Hsiao-ChungLin. An e_cient network intrusion detection.Computer communications, 33(4):477-484, 2010.
[17] Sapna S. Kaushik and Dr. Prof. P. R. Deshmukh.Detection of attacks in an intrusion detectionsystem. International Journal of ComputerScience and Information Technologies, 2(3):982- 986, 2011.
[18] Ciza Thomas. Application of machine learning for intrusion detection: Challenges and solutions,2013.
[19] Chih-Fong Tsai, Yu-Feng Hsu, Chia-Ying Lin, and Wei-Yang Lin. Intrusion detection by machinelearning: A review. Expert Systems withApplications, 36(10):11994-12000, 2009.
[20] Chenfeng Vincent Zhou, Christopher Leckie, and ShanikaKarunasekera. A survey of coordinatedattacks and collaborative intrusion detection.Computers & Security, 29(1):124-140, 2010.
[21] S. Axelsson, Research in Intrusion-Detection Systems: A Survey, tech. report TR-98-17, Dept. Computer Eng.,Chalmers Univ. ofTechnology, 1999.
[22]Vieira, K. Schulter, A. Westphall, C.B. Westphall, C.M. ―Intrusion Detection for Grid and Cloud Computingǁ IEEE computer society,vol 12, issue 4, pp. 38 – 43,2010.
[23] Gruschka N, Iancono LL, Jensen M and Schwenk J, _On Technical Security Issues in Cloud Computing', _09 IEEE InternationalConference on Cloud Computing, pp 110-112, 2009.
[24] H. Takabi, J. B. D. Joshi and G. Ahn, Security and Privacy Challenges in Cloud Computing Environments, Security & Privacy, IEEE, 8 , pp. 24-31,2010.
[25] Stephen M. Specht, Ruby B. Lee," Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures". In Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems,2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543-550, September 2004.
[26]"LuitInfotech: What is Cloud Computing", Download, pp1 http://www.luitinfotech.com/kc/what-is-cloud-computing.pdf (accessed in Feb 2013).
[27] Sebastian Roshke, Feng Cheng, ChristophMeinel, "Intrusion Detection in the Cloud". In Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp. - 729-734, IEEE, October 2009.
[28] RohitBhadauria, SugataSanyal, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. In International Journal of Computer Applications 47(18): pp 47-66, June 2012.
[29] A. M. Lonea, D.E. Popescu, H Tianfield , " Detecting DDoS Attacks in Cloud Computing Environment", INT J COMPUT COMMUN, ISSN 1841-9836, Feb 2013.
[30] DimitriosZissis, DimitriosLekkas "Addressing cloud computing security issues", University of the Aegean, Syros 84100, Greece –IEEE Dec 22, 2010.
[31] Minqi Zhou, Rong Zhang, Wei Xie "Security and Privacy in Cloud computing: A Survey" sixth International Conference on Semantics, 2010.
[32] Yonghua You, Mohammad Zulkerine, Anwar Haque, " A distributed Defense framework for flooding-based DDOS attack" Third International conference on Availability and security, 2008