International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7017(O)
Issue 2, Volume 3 (March 2015) ISSN: 2349-7009(P)
www.ijiris.com

THRESHOLD BASED APPROACH TO DETECT DDOS ATTACKS IN CLOUD

Baldev Singh
Research Scholar
Punjab Technical University, India

Dr. S.N. Panda
Chitkara University
Rajpura, India

Dr. G.S.Samra
Lyallpur Khalsa College
Jalandhar, India

Abstract— Cloud computing environment is very much prone to intrusion attacks due to modern-days new attacks and hence security of cloud computing is very much required. People will move towards cloud services until and unless they are not having full reliance in its security. Although various measures are taken place from time to time but still various attacks like DDOS attacks are glaring. Hence Multiple Dynamic Thresholds based DDOS attack detection mechanism is proposed as statistical algorithms are more stable.

Keywords— Threshold, DDOS Attack, Static Threshold, Virtualization, Dynamic Threshold, Intrusion Detection

I. INTRODUCTION

Cloud computing technology has emerged in modern times through which storage, network and computation is offered as a service to the cloud users. The cloud users hold and release the services as per requirement. It is a pay per use model, where users pay only for the resources they need. The National Institute of Standard and Technology (NIST) defines Cloud Computing as the model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., Networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [16].Cloud Computing services comprise three different service models, namely Infrastructure-as-a Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Cloud Computing is one of the fastest growing service models on the Internet. Various large scale IT service providers, like Amazon and IBM, share their data centers, by using virtualization concepts, for the public usage of their computational resources. By using cloud computing, the users of cloud can minimize many startup financial overheads as well as obtain an increase in the availability and scalability for their cloud-hosted applications.

II. VIRTUAL MACHINES

Virtualization is critical component being used in cloud computing. It is a key element that simplifies the service delivery of a set of dynamically scalable resources such as storage, software, processing power and other computing resources to the cloud users which could be accessed over the Internet on demand. A user needs only a browser and an Internet connection to use these resources. Virtual machines (VMs) are created within a virtualization layer [31]. A cloud is built up of numerous host machines these physical machines then run multiple virtual machines, which is what are presented to the end-users. There is virtualization software available that can emulate an entire computer that means single computer can perform as though it were actually 50 computers (e.g.). With the use of such kind of software one might be able to migrate from a data center with thousands of servers to one that supports as few as a couple of hundred.

Virtual machines are only limited in the way that their specifications cannot exceed that of their host machine. A virtual machine is a software implementation of a computing environment in which an operating system (OS) or program can be installed and run. The virtual machine typically emulates a physical computing environment, but requests for CPU, memory, hard disk, network and other hardware resources from the host machine that are managed by a virtualization layer which translates these requests to the underlying physical hardware. Researchers get the ability to test applications, their deployments and upgrades more efficiently by using VMs. They don't need to have multiple OS and installation configurations.

III. CLOUD SECURITY ISSUES

Cloud computing security is one significant issue in the usage of cloud services. Cyber attacks against large internet ventures keep on rising and they directly affect the cloud users. Cloud customers (organizations) are questioning the security of moving their computational assets toward the cloud. These improper operations are generally conducted for a number of reasons. Financial gain can also be a motivation to steal valuable information from sensitive organizations such as those in the banking sector. Cyber surveillance operations typically conducted to gather information about financial or industrial adversaries are some of the new trends over the internet. Existing network security mechanisms face new challenges in the cloud such as DDOS attacks [14], virtual machine intrusion attacks and malicious user activities. Hence, new security methods [27], [22] are required to increase users' level of trust in clouds. Presently, cloud service providers implement data encryption for the data centers, virtual firewalls and access control lists. Cloud Security Alliance[7] identify the following threats in the initial document:

© 2014-15, IJIRIS- All Rights Reserved

- *Abuse and Nefarious Use of Cloud Computing*
- *Insecure Application Programming Interfaces*
- *Malicious Insiders*
- *Shared Technology Vulnerabilities*
- *Data Loss/Leakage*
- *Account, Service & Traffic Hijacking*

IV. DDOS ATTACK

A DDOS attack is a malicious attempt to make the resources (a server or a network resource) unavailable to the users usually by blocking or interrupting the services of a host machine to the Internet. DDOS attack took place by using many computers and many Internet connections often distributed globally. Following figure shows a simple DDOS attack scenario [15],[17] in which multiple attacking computers are sending streams of malicious packets to victim machine.

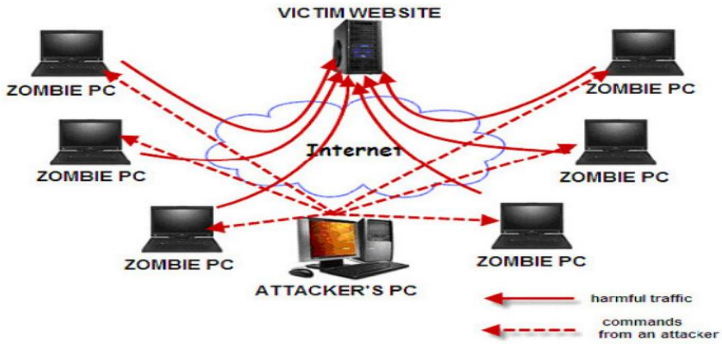

Fig.1: Distributed Denial-of-Service Attack Scenario

DDOS attacks attempt to perform the following malicious operations:

- Control legitimate network traffic by flooding the network with malicious traffic.
- Deny access to a service by way of disrupting communication between legitimate sender and receiver,
- Block the access of a particular service or an individual.

DDOS attacks lead to disruption of services in cloud and is considered as one of the important intrusions in cloud computing. Intrusion detection and prevention systems taxonomy attacks are classified as outside attacks and inside attacks [20], [25]. The attacks that come from external origins are called outsider attacks. Insider attacks, involve unauthorized internal users attempting to gain and misuse non-authorized access privileges. Intrusion detection is the mechanism of monitoring computers or networks for unauthorized entry, activity or file modification. Attacks may be treated as incidents. Although many incidents are malicious in nature, many others are not; for example, a person might mistype the address of a computer and accidentally attempt to connect to a different system without authorization.

There is an established underground cyber criminal economy which works to achieve their private individual goals best known for their keen interest in spying or for competitive monetary gains, motives that are possible by the use of disruptive technologies like DDOS attack. Thus making the science of DDOS attacks ever evolving and growing in current context in such a manner that a continuous monitoring with sophisticated watchdog capabilities is required as these attacks continues to create online outrages, customer inconvenience and reputation damages across all industries and geographies. The best known victims of recent moves of these DDOS attacks [24], [26] and those who have been successfully being able to mitigate such attacks can never get a sound sleep as it is apparent from current incidences of this attack globally.

V. VARIOUS DENIAL OF SERVICE ATTACKS

DDOS attack results to disruption of services in cloud and is considered as one of the important intrusions in cloud computing [5], [30]. The DDOS attacks (http://www.isi.edu/~mirkovic/bench, 2015) can be classified as under :

Bandwidth Attacks: These Attacks are anticipated to overflow and consume available resources of the victim (for example: network bandwidth). Some examples of Bandwidth chocking in context of DDOS attacks are TCP SYN Flood, UDP Flood and ICMP Flood [21], (Retrieved December 13, 2014, from http://www.carbon60.com/the-truth-about-DDOS-attacks-part-1).

© 2014-15, IJIRIS- All Rights Reserved

Protocol Attacks: Protocol Attacks exploit a specific feature or implementation bug of some protocol installed at the victim for the purpose of consuming maximum amount of its resources to take benefit of protocol intrinsic design. All these attacks require a lot of attackers (zombies) and are mitigated by changing the protocol features. Some examples of popular protocol attacks Smurf Attack, UDP Attack, ICMP Attack, SYN attack, Attack using DNS systems, CGI request attack, Attack using spoofed address in ping, Authentication server attack etc.

Software Vulnerability Attacks: Software Vulnerability Attacks allows an attacker to exploit a software program design flaw that may be a Land attack, Ping of Death or Fragmentation etc. Vulnerability in software means a weakness which permits an attacker to lessen a system's information assurance.

DDOS ATTACK STATISTICS

- Attackers are getting sophisticated. They are changing their tools and techniques to intrude into the network of others and attack intentionally. Following are the factors that show light on attack sophistication of the intruders:
- Intruders are doing their best to apply multi-vulnerability attack mechanism to target all layers of the victim's IT infrastructure. The layers namely the network, servers, and application layers.
- Intruders are more concentrating over DDoS tools to focus on applications rather than distributed denial of service (DDoS) attack tools that focused on networks.
- Intruders are using "low & slow" attack mechanism keeping in mind to misuse the application resource rather than resources in the network stacks.
- Intruders are more focusing on evasion techniques to avoid detection and mitigation including SSL based attacks, changing the page request in a HTTP page flood attacks etc.

The following table shows a brief statistics of various attacks.

TABLE 1: DDOS ATTACK STATISTICS (RETRIEVED DECEMBER 05, 2014, (TRIPATHI,GUPTA,MISHRA & VELURU, 2013)

Year	Attack Description
2014	114 percent increase in average peak bandwidth of DDOS attacks in Q1 vs. Q4 2013. The Media and Entertainment industry was the target of the majority of malicious attacks. (Retrieved December 05, 2014 from http://www.akamai.com/html/about/press/releases/2014/press-041714.html)
2013	DDOS attack on stock exchange websites in London.
2012	DDOS Attack on Canadian Political Party Elections and on US and UK Government Sites
2011	DDOS attack on Sony.
2010	DDOS—December 3-5, 2010 on PayPal.
2009	DDOS flooding attacks on South Korea and the United States in July 2009 against government news media and financial websites.
2008	DDOS Attack on BBC, Amazon.com and eBuy.
2007	Estonia Cyber Attack
2006	Target US Banks for financial gain.
2004	Attack on SCO Group website to make it inaccessible to valid users.
2003	Attack on SCO and Microsoft.
2002	DDOS flooding attack thru Domain Name System (DNS) service.
2001	DNS servers attack as reflectors. DOS attack on Irish Government's Department of Finance server. The target was Register.com
2000	One of the first major DDOS flooding on Yahoo

Following components/processes are required to ensure high availability of services for the cloud customers that means proper scrubbing centers are required for this purpose either at cloud service provider end or user end which is not an easy task.

- *Detection and Monitoring System.*
- *Threat correlation services.*
- *Threat alert system.*
- *Threat identification service with false positives recognition.*
- *Threat rate of change.*
- *Threat severity analysis.*
- *Threat heuristics at every layer.*

Hence, when a centralized data cleansing stations are deployed having all possible capabilities as mentioned above where traffic is scrutinized and mischievous traffic (DDOS, known susceptibilities and exploits) are moved or absorbed. There is normally an assumption that a volumetric attack bandwidth consumption can be overcome by adding more and more bandwidth, and swallow all data traffic thereby continuing the services, but it can happen for how much and how long is a question.

© 2014-15, IJIRIS- All Rights Reserved

Since , the target of the any DDOS attackers is normally to block or oversubscribe a resources in such a way that it leads to degraded service performance time, long response time matching the demand of processing the incoming workload remains a constant headache. Many methods have been evolved over a considerable time now and all these methods or technologies that claim to safeguard us from DDOS attacks also consider the various possible correlations that might be working to advantage of the attackers.

VI. RELATED WORK

Lot of work has been done by this domain experts related to solutions for providing security and mitigation of attacks in cloud network. Cloud based networks and services are prone to suffer from malicious attacks because of their inherent characteristics of being accessible globally any time and also due to the frequent changes in topology and development of Internet of things as well as because of landscape nature of Internet. Mainly it is the denial of service attacks that makes the service unavailable to its intended cloud users. Two techniques can be used in selecting the appropriate threshold that differentiates between the malign network traffic and abnormal network traffic. These techniques are based on the *static threshold value* and *dynamic threshold value.*

Various threshold based techniques [13], which can be used to detect intruders or malicious behavior in the cloud network, are reviewed. These techniques have their own pros and cons. To realize this field of IDS we stare at what each technique holds in its favour and what trade-offs it must make to achieve its goals particularly to make out the abnormal behavior which seems to be DDOS attack.

Static threshold based intrusion detection system was propounded by Kim et al. (2004), Gates and Damon (2005), Leckie et al (2002) and Faizal et al (2009). Network IDS technique proposed by [25] has used the concept of static threshold although dynamic threshold is better solution. The threshold is used to differentiate between normal traffic and abnormal traffic in the network. This threshold value is acquired by using observation and experimental technique [13] and the verified by using statistical process control approach. The main merit of this approach is " Absolute threshold values easy to implement for detection, Low computational complexity". Demerits include:`` Fix value range is never close to real systems that changing every day, this method will never be able consider differential or cumulative threshold for giving response to adversity in real time".[12].

Dynamic threshold based technique is more complex than the technique based on static threshold. Dynamic threshold value is based on training or priori knowledge of the network activity, after that the threshold is selected [12]. According to Faizal et a., It is time consuming process to generate priori knowledge required for generating the dynamic threshold. Their study is based on Fast attack detection mechanism. Shahrin et al. has proposed a framework of fast attack detection. The framework is based on the fast attack detection from two perspectives which are Attack Perspective and the Victim Perspective. Faizal et al. use the framework of fast attack detection at the earliest as they are more hazardous for the network. Their technique is based on the victim perspective of fast attack detection. According the [11] fast attack can be defined as an attack that make connections within few seconds and it uses the huge volume of packet. The work for fast attack detection of [11] is mainly based on distributed denial of service attack. The selection of right feature selection is important for detection of attack. The features may also include some extraneous features that are to be treated as spurious features and inadvertently increase the computational issues which include memory space, time and CPU cycle and hence may cause decrease of accuracy of attack detection. The features used by [11] in the detection of fast attack includes Timestamp (time to send the packet), Duration of connection, IP address of host, Connection protocol, Status flog of connection, Source and destination services and number of connections in Attack-Victim connection. The research work of Faizal et al. is based on static threshold to detect attacks mainly fast attack and has considered not other main protocols like UDP and ICMP for intrusion detection.

Sanchika Gupta [18] proposed the profile based dynamic threshold based intrusion detection. They have proposed the concept of privileged domain in which each virtual machine is in privileged domain. In this architecture, each virtual machine in the cloud network is filtered on their IP address based in the privileged domain. The attacks are detected on the basis of profile of each virtual machine (VM) in the cloud network. VM profile is beneficial to detect attacks as traffic of VM is not detected for each attack, only those attacks are detected which are frequent in nature. Although [18] claimed the dynamic threshold profiling but no factor analysis for signature design is used and the proposed rank based detection is irrelevant.

L. Jun-Ho et.al. has presented the research work in the [12] is based on intrusion detection at multiple levels. As above research work has proposed intrusion detection on basis of fast attacks and slow attacks, the later is based on security implementation at multiple levels. [12] Authors proposed different anomaly levels in cloud environment that are authentication, authorization and accounting (AAA). They also proposed three security levels for effective intrusion detection system that are High, Medium and Low.

© 2014-15, IJIRIS- All Rights Reserved

In case of High level of security requirement, they has suggested that- the patterns of all the known attacks are to be considered and the requisite rules for higher level security are to be implemented. They were of the opinion that when the user access the cloud environment first time, the multi level intrusion detection system (IDS) must judge the anomaly level of the user. For judgment of anomaly level, [12] authors suggested various parameters like vulnerable ports attack, IP address coverage of user, attack success possibilities, attack occurrence possibilities etc. They suggested risk points for different security groups. If the risk points are greater than six, the anomaly level is of High level, risk points between 3-5 (both inclusive), the anomaly level is of medium level and for risk points 0-2, the anomaly level is of low level and accordingly IDS is required to be imposed.

The main demerits of this approach are:

-Enormous log entries so not cost effective;
-Lots of rules for Ranking of risks and file monitoring modules require high consideration for absolute solution but reduction in resources will be a question.
-Each VM in one security group (H/M/L). Migration of VM from one security group to another is only judgment basis.

Hai Jin et al. proposed VMM (virtual machine monitoring) based research work. This virtual machine monitor in cloud computing environment has the concept of customizable defense system known as VMFence which is used to monitor network flow and file integrity and suggested a network defense and protection of file integrity in the cloud environment. They have implemented VMFence on Xen (open source VM platform) for intrusion detection and prevention system in cloud computing environment [24]. This system monitors the attack patterns coming through all VMs that are connected to the privileged machine. The main demerits of this approach are:

-Extra computationally complex as it monitors the attack patterns coming thru all VMs that are connected to the privileged machine.
-Due to this heavy workload on privileged machine, the n/w will chock and packet drop rate increases

ESSENCE OF THE REVIEW LITERATURE

It is complex to detect the DDOS attacks as well as all other such kinds of attacks of every virtual machine.

- *Dynamic systems like cloud or adversity causing systems cannot work on such single threshold and detection decision making may be faulty.*
- *It cannot work on multi-range threshold systems as the range may be discrete or continuous and may be changing with time.*
- *Difficult to calculate accurately as ranges may change with pattern which is difficult to realize.*
- *Threshold may go wrong due to erratic behavior of matrices used.*
- *Statistically cannot handle extreme high and low values that may lead to wrong calculations.*

Extensive efforts have been made to understand, detect and prevent these attacks. Since it is a continuously evolving as technology, new ways are found by anti development sources to compromise the Cloud based Systems, therefore methods that are based on single, multi range thresholds for detection, require constant upgradation as well refinement in terms of the algorithms for accuracy and robustness. The algorithms reviewed for detection of DDOS attack are not always been numerically stable.

VII. PROPOSED FARMEWORK

The current intrusion detection systems mentioned in the review literature, overlooks certain aspects of calculating the threshold for identification of subspace set of abnormal behavior with the whole pattern of VM profile and this is based only frequency calculation happening in particular set of time line, which is not capable of further mathematical treatment or insight and it is more useful in qualitative cases, however, it makes more sense, if relative frequency based threshold could have been used which would have also considered the total outcome of normal and abnormal events in the VM profile. It would be more accurate to consider those methods that would fine in extreme cases when values are either too large or too small or the dataset is skewed due to particular pattern of events.

In our research work we intend to analyze methods that can deal with skewed datasets (the ratio of data-row of normal behaviour [benign traffic] to abnormal behaviour [malignant traffic] rows in the profiling session of virtual machines) (trace files or profile files) for detection of DDOS attacks, since the thresholds cannot be static in nature (the statistical behaviour) in any way in cloud environment for parameters that are critical to analyse for identification of DDOS Attacks. The signature based and anomaly based DDOS mechanism is proposed which encompasses the use of dynamic and multi threshold based algorithmic approach. There is ample scope of the proposed solution in the cloud computing environment as network attacks are glaring day by day. Our research will focus on early detection of network attacks, robust and minimum complex system.

© 2014-15, IJIRIS- All Rights Reserved

VIII. CONCLUSION

On the basis of review literature done in the context of the DDOS attack we can anticipate that there will be increase in the frequency of the DDOS attacks due to multifold increase in the online activities and Internet of things. Both the internal and external anatomy of the data center matters, how it is structured architecturally to measure the volume of traffic is the main critical point, if somehow the intruders are able to launch a slow attack it must be detectable or if it is a sudden flood of packets then we must be able to mitigate the flood to have attack-free traffic. Continuous monitoring of cloud network is required. Hence, the thresholds to find inflection points where the traffic changes to malicious are very much necessary so that a proactive approach be applied in detecting the DDOS attacks.

REFERENCES

[1] Dit-Yan Yeung,User Profiling for Intrusion Detection Using Dynamic and Static Behavioral Models *Springer Berlin Heidelberg,* 2002
[2] Ahmed Patel et. al., "An intrusion detection and prevention system in cloud computing: A systematic review", *Journal of Network and Computer Applications (2012), http://dx.doi.org/10.1016/j.jnca.2012.08.007*
[3] Shicong Meng; Iyengar, Arun K.; Rouvellou, I.M.; Ling Liu; Kisung Lee; Palanisamy, B.; Yuzhe Tang, "Reliable State Monitoring in Cloud Datacenters," Cloud Computing (CLOUD), 2012 IEEE 5th International Conference vol., no., pp.951,958, 24-29 June 2012doi: 10.1109/CLOUD.2012.10
[4] Bao-Tung Wang; Schulzrinne, Henning, "An IP traceback mechanism for reflective DoS attacks," Electrical and Computer Engineering, 2004. Canadian Conference on, vol.2, no., pp.901, 904 Vol.2, 2-5 May 2004 doi: 10.1109/CCECE.2004.1345260
[5] B. B. Gupta, R. C. Joshi and M. Misra, "Defending against Distributed Denial of Service Attacks: Issues and Challenges," *Information Security Journal: A Global Perspective, Vol. 18, No. 5, 2009, pp. 224-247.*
[6] "CERT Advisory: SYN Flooding and IP Spoofing Attacks," CERT® Coordination Center Software Engineering Institute, Carnegie Mellon, 2010. http://www.cert.org/advisories/CA-1996-21.html
[7] Cloud Security Alliance, March 2010 —Top Threats to Cloud Computing at (http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf)
[8] Faizal M.A., and Zaki M.M., and Shahrin S., and Robiah Y., and Rahayu S.S., (2010) Statistical Approach for Validating Static Threshold in Fast Attack Detection. *Journal of Advanced Manufacturing.*
[9] I.S. Institute, DDOS Attack Categorization, University of Southern California. DDOS Bechmarks; (http://www.isi.edu/~mirkovic/bench/), 2015.
[10] Jagadeeshraj.V.S , Lijoy C. George , Thenmozhi.S, "Attaining Pre-Eminent Cloud Security Using Intrusion Detection Systems, *International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 2, February 2013.*
[11] Kelly Beardmore, "The Truth about DDoS Attacks: Part 1, TheCarbon60 Blog. - http://www.carbon60.com/the-truth-about-DDOS-attacks-part-1/Nov.21, 2013.
[12] L. Jun-Ho et.al. "Multi-level intrusion detection system and log management in cloud computing," *Proceedings of the13th International Conf. pp. 552–555, Feb. 2011*
[13] Mohd Faizal Abdollah, Mohd Zaki Masud, Shahrin S., Robiah Y. , Siti Rahayu S. "Threshold verification using Statistical Approach for Fast Attack Detection" *Intl. Journal of Computer Science and Information Security, Vol.2, No 1, 2009.*
[14] Monowar H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya and J. K. Kalita. Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions . *The Computer Journal, 2013.*
[15] Nathalie Weiler, Computer Engineering and Networks Laboratory (TIK), "Honeypots for Distributed Denial of Service Attacks", *Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002.*
[16] Peter Mell and Tim Grance, October 7, 2009 The NIST Definition of Cloud Computing version 15, National Institutes of Standards and Technology (NIST), Information Technology Laboratory -
[17] R. C. R. Bhadauria, N. Chaki, and S. Sanyal, "A survey on security issues in cloud computing, 2011" (http://arxiv.org/abs/1109.5388).
[18] Sanchika Gupta, Padam Kumar, and Ajith Abraham., A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment, *International Journal of Distributed Sensor Networks* , Volume 2013 (2013), Article ID 364575
[19] Shicong Meng; Iyengar, Arun K.; Rouvellou, I.M.; Ling Liu; Kisung Lee; Palanisamy, B.; Yuzhe Tang, "Reliable State Monitoring in Cloud Datacenters," Cloud Computing (CLOUD), 2012 *IEEE 5th International Conference on , vol., no., pp.951,958, 24-29 June 2012doi: 10.1109/CLOUD.2012.10*

© 2014-15, IJIRIS- All Rights Reserved

[20] S. M. Specht and R. B. Lee, "Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures," *Proceedings of the International Workshop on Security in Parallel and Distributed Systems, San Francisco, 15-17 September 2004, pp. 543-550.*

[21] Song Ning; Qiu Han, "Design and implementation of DDOS attack and defense testbed," Wavelet Active Media Technology and Information Processing (ICWAMTIP), 2012 *International Conference on , vol., no., pp.220,223, 17-19 Dec. 2012 doi: 10.1109/ICWAMTIP.2012.6413478*

[22] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, 2011.*

[23] Shweta Tripathi, , Brij Gupta, Ammar Almomani, , Anupama Mishra, Suresh Veluru; "Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDOS) Attacks" *Journal of Information Security, 2013, 4, 150-164.*

[24] Udhayan, J.; Anitha, R., "Demystifying and Rate Limiting ICMP hosted DoS/DDOS Flooding Attacks with Attack Productivity Analysis," Advance Computing Conference, 2009. *IACC 2009. IEEE International, vol., no., pp.558, 564, 6-7 March 2009 doi: 10.1109/IADCC.2009.4809072*

[25] Vasanthi, S.; Chandrasekar, S., "A study on network intrusion detection and prevention system current status and challenging issues," *Advances in Recent Technologies in Communication and Computing (ARTCom 2011), 3rd International Conference on* , vol., no., pp.181,183, 14-15 Nov. 2011 doi:10.1049/ic.2011.0075

[26] Xie Chuiyi; Zhang Yizhi; Bai Yuan; Luo Shuoshan; Xu Qin, "A Distributed Intrusion Detection System against flooding Denial of Services attacks," Advanced Communication Technology (ICACT), 2011. *13th International Conference on , vol., no., pp.878,881, 13-16 Feb. 2011*

[27] Xia Chun-Tao; Du Xue-Hui; Cao Li-Feng; Chen Hua-Cheng, "An Algorithm of Detecting and Defending CC Attack in Real Time," Industrial Control and Electronics Engineering (ICICEE), *2012 International Conference on* , vol., no., pp.1804,1806, 23-25 Aug. 2012 doi: 10.1109/ICICEE.2012.477

[28] Yuxin Ding , Dit-Yan Yeung, User Profiling for Intrusion Detection Using Dynamic and Static Behavioral Models, *Springer Berlin Heidelberg*, 2002

[29] Priyanka P. Kukade; Geetanjali Kale," Survey of Load Balancing and Scaling approaches in cloud " *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)* Volume 4, Issue 1, January-February 2015

[30] Felix Lau Simon , Stuart H. Rubin , H. Smith , Trajkovic , "Distributed Denial of Service Attacks"; http://www2.ensc.sfu.ca/~ljilja/papers/smc00_edited.pdf, 2000.

[31] H. Jin, G. Xiang, D. Zou, "A VMM-based intrusion prevention system in cloud computing environment,"*The Journal of Supercomputing, pp. 1–19, 2011.*

[32] "Denial-of-Service (DoS) Secured Virtual Tenant Networks (VTN)" Top Threats to Cloud Computing V1.0 by *Cloud Security Alliance.* http://www.necam.com/docs/?id=0078a286-d99d-4d2c-ab54-d18814b59dd7

© 2014-15, IJIRIS- All Rights Reserved