ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
August 2015,
Vol. 8, No. (2):
Pgs. 110-120

Various Techniques of DDoS Attacks Detection and Prevention at Cloud: A Survey

DALIMA PARWANI[1], AMIT DUTTA[2], PIYUSH KUMAR SHUKLA[3] and MEENU TAHILIYANI[4]

[1]Department of Computer Science, Sant Hirdaram Girls College, Bhopal, 462030, India.
[2]Computer Science & Application, Barkatullah University, Bhopal, 462001, India.
[3]Computer Science & Engineering, University Institute of Technology, RGPV,
Bhopal, Airport Bypass Road, Gandhi Nagar, Bhopal 462033, India.
[4]Department of Computer Science, Sant Hirdaram Girls College, Bhopal, 462030, India.

(Received: May 06, 2015; Accepted: June 25, 2015)

ABSTRACT

Cloud Computing is one of the fastest growing concept of transmitting the data or storing data so that the user can access data from anywhere. But with the advancement of growing new technology various challenges have emerged such as security from various attacks, computational cost and power consumption. One of the major issues is the Distributed Denial of Service Attack. It is a type of attack where a multitude of compromised systems start attacking on a single target that enables denial of services for the user of the targeted system. Hence, various techniques are implemented for the detection and prevention of these attacks; some of the techniques work better while some have issues, concerns and problems. In this paper, a complete survey and analysis of various Distributed Denial of Service Attack detection and prevention technique is analyzed and discussed so that on the basis of issues surfaced, a new, reformed and efficient technique is implemented for the detection and prevention of Distributed Denial of Service Attack especially in Cloud Computing System.

Key words: Cloud computing; Denial of Service; Distributed Denial of Service; Security; Detection; Prevention.

INTRODUCTION

Cloud Computing is an evolving paradigm that is growing rapidly and is a modern model that is intended to provide suitable, on-demand, network access to a common group of configurable computing resources “as a service” on the Internet for fulfilling computing demands of the users. Services on the Cloud are delivered by the Internet. Due to this security and privacy of Cloud resources, data and offered services are the main concerns in cloud. So many security issues come when we use cloud computing - First is the Security issue faced by cloud computing providers and the second is the issue faced by the cloud customers. In most of the cases, the provider must make sure that their framework is secure and that their clients’ data and applications are protected. On the other hand customer also wants to ensure that the provider has exerted proper security actions to protect their information. Cloud computing also provides benefits by bettering the capabilities of

any business organization without reinvesting in new framework, training employees, and user and to provide licensing of new software.

So many traditional attacks affect the working of cloud computing, these attacks affect the integrity, confidentiality, and the availability of Cloud resources and existing services and are present at the network layer. These attacks are DNS Poisoning, Denial of Service(DoS), Distributed Denial of Service(DDoS), IP Spoofing, man-in-the-middle attack, port scanning, Address Resolution Protocol (ARP) spoofing, Insider attack, Routing Information Protocol(RIP) etc.

To evade these issues, most of the Cloud providers use firewalls. Firewall is the border access points of system and it provides protection at first place i.e., at the border of any environment or network. Since firewall detects the network packets only at the boundary of any network, then insider attacks cannot be found using this. Some attacks which belong to DoS or DDoS are too difficult to detect by using usual firewall. As a result of that, use of firewalls to block all the intrusions is not an efficient solution. Another method we can employ is to combine Cloud computing with network based detection system (NIDS). NIDS do the function to au-courant system and it adds preventive layer which provide security by detecting attacks which induces our system. Two techniques can be used in NIDS. One is the signature based detection method that can be used to detect known attacks efficiently. The other approach can be anomaly detection method that finds the behavior of packet or user is malicious or not. NIDS efficiency depends on the parameters used in the detection technique, its position in the network means where NIDS is placed i.e., in front or at back end, how system arranges or configures centralized or distributed environment.

Types of Cloud Computing

Delivery Model

Delivery model is of four types in Cloud Computing, they are:

Public cloud

In public cloud computing, the cloud provider makes the resources accessible to the customers over the Internet which is public network. Usually the documents of the company which uses the public cloud are stored external to its location by a third party whom they trust. This increases the risk of data privacy and security because of cloud infrastructure in which computers, network and storage are placed outside the company's firewall.

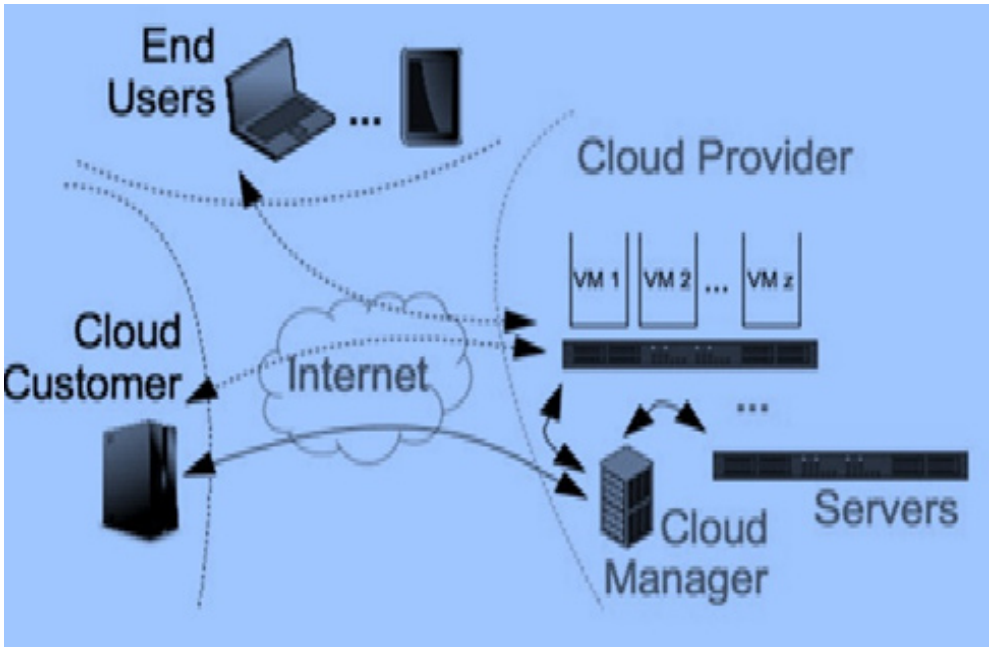

Fig. 1: Secure Cloud Computing

In the private cloud, the organization allows own resources over its private network. The company owns the services, resources and also defines which users can access it. The security risks are also reduced because all things are managed inside the enterprise or organization. Firewall allows a fair use of the applications and the network bandwidth.

Hybrid cloud

Hybrid cloud is a computing platform, which combines or we can say make connection between private cloud and public cloud. It is deployed by organizations, which do not want to put all things in the external cloud (i.e., public cloud) while hosting some servers in their own internal cloud infrastructure. The provider of the Cloud is able to process applications which can work in between those boundaries.

Community cloud

A community cloud is a platform, which allows companies to share resources and infrastructure over a common cloud environment. The condition for this is that they should belong to same industry and they do the same type of operations. It is prepared and provided by one company and used by the others or provided by a third party over the Internet.

Service Model

Software as a Service (SaaS)

This is the most important model from user's point of view. In this model, cloud provider installs and operates different application software's in the cloud environment. The cloud users can access these software's from cloud clients but do not directly access the infrastructure of Cloud as well as platform on which the particular application is running i.e. , the users can access the software online and can store the data back in the cloud. It eliminates the need of installing the application on the user's own computers. This feature provides simplified maintenance and support for different levels of user accountability [1].

Platform as a Service (PaaS)

It is another application delivery model which provides platform or we can say: all the necessary resources to run any application without installing or downloading it. This service includes design, development, hosting, testing and deployment for any application or software. PaaS also provides support for the creation of user interface which is based on HTML or JavaScript.

Infrastructure as a Service (IaaS)

It is an application in which limited number of resources is easily allocated to large number of users. Infrastructure refers to the operating system and its virtualization that is how efficiently it manages resources without administering background details. Dedicated CPU is allocated; moreover, they access the virtual memory conferring to their accountability in cloud environment.

SaaS and PaaS are used to provide application services to the user, where as IaaS is used to provide hardware services so that organization can lay whatever they want to nail onto it.

Rationalie

In July 2009 in Japan, an effort called the Global Inter-Cloud Technology Forum (GICTF) was launched with the stated goal of "We aim to promote

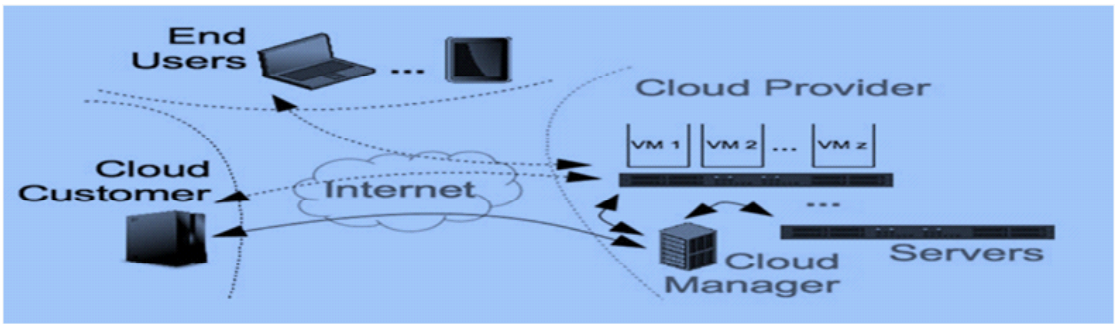

Fig. 2: Deployment models of Cloud

standardization of network protocols and the interfaces through which cloud systems interwork with each other, and to enable the provision of more reliable cloud services than those available today". As of mid-2012 they have over 85 member companies and have published proposed use cases as well as technical documents.

In July 2010 in France the First IEEE International Workshop on Cloud Computing Interoperability and Services (InterCloud 2010) was held bringing researchers together and yielding many published papers. The workshop has become an international research series, with InterCloud 2011 held in Turkey, InterCloud 2012 held in Madrid, and InterCloud 2014 held in Boston.

In February 2011 the IEEE launched a broad cloud computing initiative IEEE Cloud Computing including a technical standards effort called P2302 - Standard for InterCloud Interoperability and Federation (SIIF). The stated goal of the working group is to produce a standard as such: "This standard defines topology, functions, and governance for cloud-to-cloud interoperability and federation. Topological elements include clouds, roots, exchanges (which mediate governance between clouds), and gateways (which mediate data exchange between clouds). Functional elements include name spaces, presence, messaging, resource ontologies (including standardized units of measurement), and trust infrastructure. Governance elements include registration, geo-independence, trust anchor, and potentially compliance and audit. The standard does not address intra-cloud (within cloud) operation, as this is cloud implementation-specific, nor does it address proprietary hybrid-cloud implementations." As of mid-2012 they have over 50 member companies and have published a Working Draft 1.0.

In mid-2011 the NIST Cloud Computing Reference Architecture was published fully describing hybrid clouds, cloud brokers, and so on. In late 2011 NIST published a whole set of Cloud Computing Technology Roadmaps including referencing the IEEE P2302 approach as an example of a future national/global federated cloud architecture.

In March 2012 "InterCloud" made the Wired Magazine Jargon Watch list.

In June 2012 at the 5th International Conference on Cloud Computing (CLOUD 2012) the IEEE announced an InterCloud Test Bed with stated goal of "The test bed will be a cloud infrastructure comprised of assets from participating universities and industry partners. It will be used to develop and test protocols that will be formalized in the IEEE P2302 interoperability standard."

In October 2013 the IEEE announced a Global Testbed initiative. The 21 cloud and network service providers, cloud-enabling companies, and academic and industry research institutions from

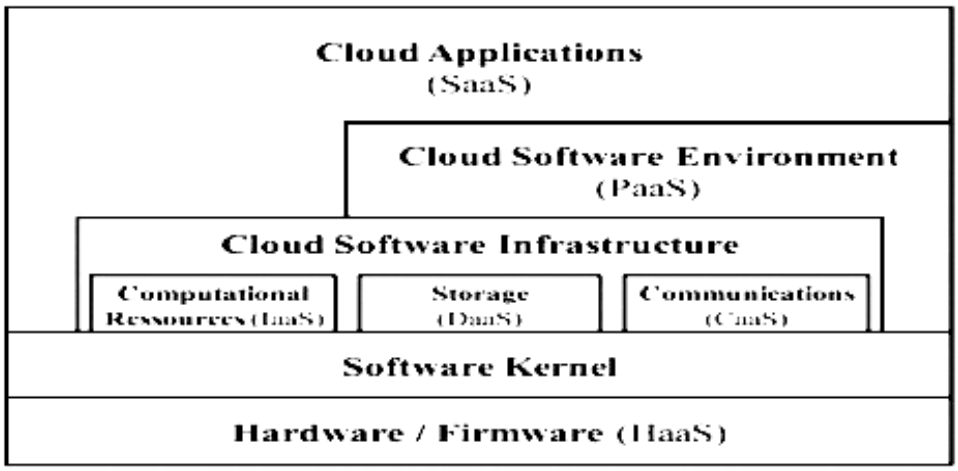

Fig. 3: Cloud Layered Model

the United States, the Asia-Pacific region, and Europe. The members have volunteered to provide their own cloud implementations and expertise to a shared testbed environment. They will also collaborate to produce a working prototype and open-source CloudOS neutral global InterCloud. As of 2014 this project is actively proceeding.

In late 2013 Cisco made their first announcement relating to the InterCloud. Their product Cisco InterCloud Fabric (ICF) allows VM migrations between public and private clouds. Cisco went on in January 2014 detailing this hybrid cloud solution, and went so far as to claim that "Cisco introduced the concept of the 'World of Many Clouds' two years ago" notably not acknowledging the work that the GICTF, NIST, or the IEEE had done.

In 2014 Cisco made another announcement Cisco revealed that it "will invest $1Bn in the next two years to build its expanded cloud business" and that "Our cloud will be the world's first truly open, hybrid cloud. The Cisco InterCloud will be built upon OpenStack for its open standards-based global infrastructure. We plan to support any workload, on any hypervisor and interoperate with any cloud" (again assuming all clouds are using Cisco's proprietary technology).

The InterCloud has yet to show real world demonstration of federation and interoperability, and challenges remain regarding security and trust, governance and legal issues, QoS, monitoring, arbitrage, and billing.

Denial of Service (DoS) Attack

When an intruder makes computer memory and resources unavailable or chock-full to handle legal request of the user and denies valid access of the server, the attack is said to be Denial-of-service attack i.e., when valid user cannot get access to server because of crowded request.

There are many types of denial of service (or DoS) attacks; certain DoS attacks neglect a completely legitimate feature, others generate unusual packets that confuse the TCP/IP stack of the machine that is trying to reconstruct the packet. We can exemplify this type of attack on a networking structure to halt a server from servicing its legal clients. Attacks are forenamed when it has too many request preferentially we can say that millions of requests are relayed to the server in an attempt to slow down, conversely, it is flooding a server with large number of invalid data or spoofed IP addresses. According to the analysis there are three types of attacks - Ping of Death, TCP SYN Flood, and the Distributed DoS.

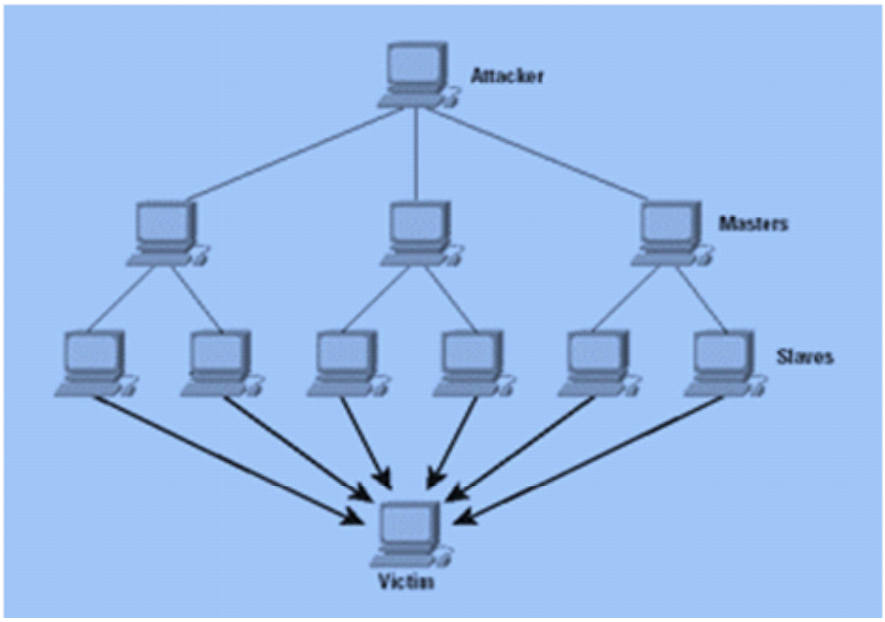

Fig. 4: DDoS Attack

In the Ping of Death Attack, host consigns hundreds or even thousands of ICMP Echo Requests; the packet size is so bulky or we can say illicit consigns to another host to affect its service moreover making him bustle due to responding so many ICMP Echo replies, and not able to service its clients.

Distributed Denial of Service (DDoS) Attacks

The main aim of DDoS [2][3] attack is to perturb and degrade the ability of server i.e., many request commissioned to the server forging it busy and incapable to serve legal request. It prevents the availability of the server for the legal users and attacker gains control over the server. Availability of the server is one more major issue in network or in cloud computing environment; if availability of server gets affected then it cannot process the legal requests. As, security is the main concern in clouds, by surmounting this obstacle we teem with a great future for clouds even bigger than the internet. We are planning to overcome one such security issue i.e., DDoS attacks which are colloquial, and can create an enormous disaster in the world of web as well as in real world.

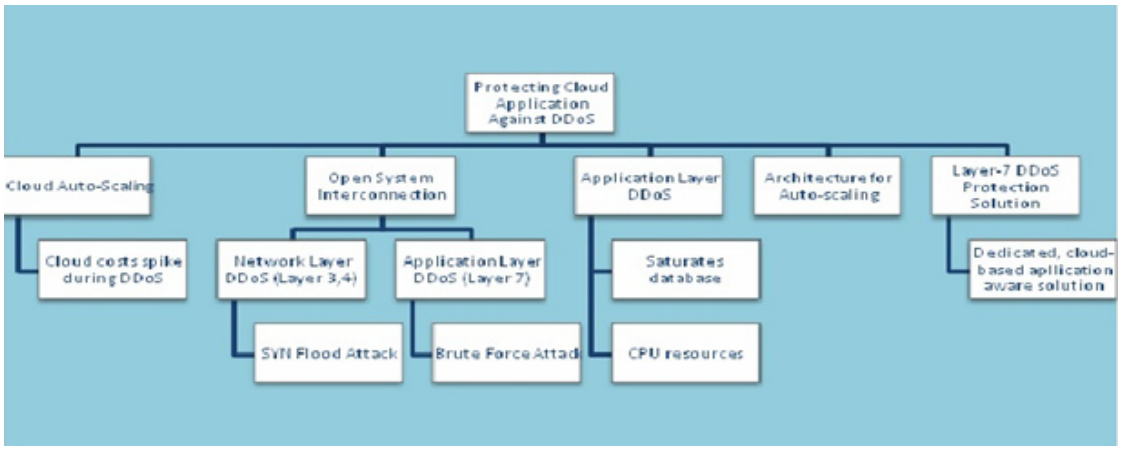

Fig. 5: Protection against DDoS

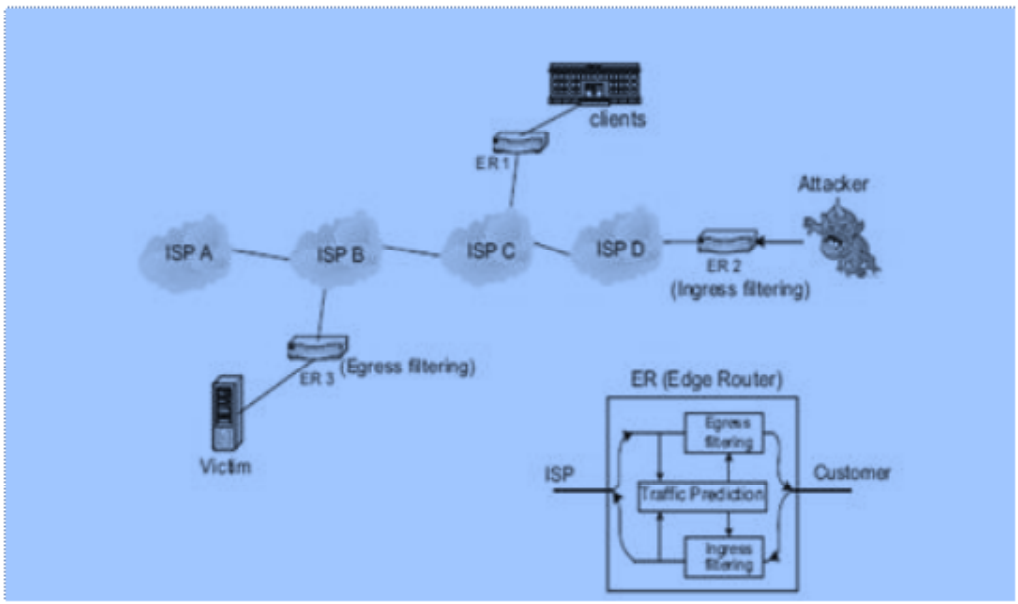

Fig. 6: Architecture of NIEF

Related Work

No.	Paper	Author	Technique Used	Issues
1.	Interconnecting Federated Clouds by Using Publish-Subscribe Service [8].	Christian Esposito, Massimo Ficco, Francesco Palmieri, Aniello Castiglione, 2013	The methodology implemented here for the interconnected federated clouds provides low computational cost as well as provides security from DDoS attacks.	Chances of Communication Delay and overhead are more as well as the framework implemented is not dynamic and feasible for DDoS attacks.
2.	InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services [14].	Rajkumar Buyya, Rajiv Ranjan and Rodrigo N. Calheiros, Springer 2010.	The proposed methodology is implemented on cloud simulator tool. The paper implements federated cloud environment for various applications.	The methodology implemented here provides performance gain but the chances of further improvement are there.
3.	A Study on Recent Approaches in Handling DDoS Attacks [15].	Debajyoti Mukhopadhyay, Byung-Jun Oh, Sang-Heon Shim, Young-Chon Kim, Cornell University Library, 2010.	Here in this paper a new and efficient approach for the Detection of DDoS attack is implemented. The paper discusses and analyses various approaches of DDoS attacks and their handling methodologies.	Implementation of these approaches is difficult to achieve.
4.	Cloud-based Security Research Testbed: A DDoS Use Case [16].	Toma´s Jirsk, Martin Husak, Pavel Celeda, Zdenek Eichler, IEEE, 2014.	The paper presents a cloud-based research testbed designed to aid network security managers. The testbed enables operators to emulate various network topologies, services, and to analyze attacks threatening these systems.	The framework is theoretical.
5.	Mitigating Distributed Denial of Service Attacks with Dynamic Resource Pricing [17].	David Mankins, Rajesh Krishnan, Ceilyn Boyd, John Zao, Michael Frentz,IEEE 2014.	Here in this paper distributed gateway based architecture is implemented for the dynamic resource pricing of Distributed Denial of Services.	Less chances of predicting attacks.

DDoS attacks are one of the major threats [4] that we are facing today. This can be launched against a web service. It is the type of attack, generated from so many dispersed hosts in the network to halt the server from servicing its clients. It also consumes all the resources provided by network, flooding the server with so many requests which flare from invalid IP addresses.

It is easy to generate this attack but hard to protect it from the wastage of resources. The main challenge in this attack is to safeguard it and the prevention crane by avoiding malicious access and dispense services to the valid or legal user.

In cloud computing environment, three major participants: the user, the service, and the cloud are there who can start the attack and against which the attacks can be launched. For all these participants in cloud, six interfaces can be assumed. They are: client to service, service to client, cloud to service, service to cloud, client to cloud, and cloud to client. A different level of security issue defines each interface.

A cloud can be private or public. Public cloud is the network which provides or sells their services to any user over the internet. But the private cloud is the network which provides its services to restricted number of people. The main objective of cloud computing is to provide easy access to computer resources and IT services; memory, resources and all services provided by cloud.

The main problem with DDoS attack is that all the source addresses are spoofed so that it is not easy to find out the real user address i.e., so many addresses are invalid, therefore, it is not easy to filter real user address from these requests.

Protecting distributed denial of service attacks

While cloud infrastructure is inherently scalable and resilient, applications deployed in the cloud are frequently hit by DDoS attacks. The users are often unaware of the unique risks, advantages and protection methods associated with protecting cloud applications against DDoS. Below are the prerequisites to be roped in when planning protection against DDoS in cloud apps. The main recommended features are:

- Application awareness
- Attack surface reduction
- False positives reduction

Literature survey

Baldev Singh, Dr. S.N. Panda, Dr. G.S. Samra proposed a new and efficient technique which is based on the concept of threshold based approach for Detection of DDoS Attacks [5]. The various packets flow in the network is analyzed on the abnormal behavior of threshold value of the packets. An efficient Multiple Dynamic Thresholds based technique is implemented here for the detection of DDoS Attack.

Dr. S. SaravanaKumar, R. SenthilKumar, R. Arun Prasad, S. Thiraviam, J. Vignesh implemented a new framework for the detection and prevention of DDoS attack in the cloud computing system [6]. Here in the paper a dynamic resource allocation based strategy is implemented to counter DDoS attacks against individual user of the cloud. A Traffic Shaping algorithm is implemented here for the analysis of resources in the cloud.

Krishna Modi, Prof. Abdul Quadir Md. Proposed a new detection and prevention system for DDoS attacks in the cloud computing system using Double TCP based mechanism and Hidden Markov Model based Architecture [7]. A Hidden Markov Model is implemented here on the cloud computing architecture for the detection and prevention of DDoS attacks in the TCP SYN Flood Attack. The proposed method uses the Double TCP Connection mechanism to ignore the spoofed packets and establish connection only with the legitimate sources and prevent any SYN Flood DDoS attack on the layer 4.

Christian Esposito, Massimo Ficco, Francesco Palmieri, Aniello Castiglione proposed an Interconnected Federated Clouds by using the concept of Publish-subscribe services [8]. Since Cloud Federation is an efficient way where multiple number of resources from various independent clouds are joined to create a single cluster. This type of clouds provides a facility to the user for multiple applications and overcomes provisioning

and scalability and also provides minimal additional cost.

Amit Khajuria, Roshan Srivastava done the analysis of the DDoS attacks and their various Defense Strategies in the cloud computing system [9]. Here in the paper analysis of various DDoS based technique are analyzed and compare the performance of various methodologies implemented for the detection and prevention of DDoS Attacks in the clouds computing system.

Patel Ankita and Fenil Khatiwala also have done analysis on various DDoS Attack detection and prevention [10]. Here in the paper a complete survey and analysis of various techniques implemented for the detection and prevention of DDoS Attacks.

G. Preetha, B.S. Kiruthika Devi, S. Mercy Shalinie implemented an autonomous agent for the detection of DDoS attacks [11]. The proposed methodology implemented here for the detection DDoS Attack provides prevention from IP Spoofing and also provides effective bandwidth and improvement in Quality of Service. The defense strength of Hop Count Filtering mechanism is obtained as 31.3% whereas the proposed Hybrid Model defense effectiveness is computed as 48.7%. Also, Adaptive Bandwidth Management (ABM) using fuzzy inference system provides sustainable bandwidth to legitimate users by providing low bandwidth share for attackers.

S. Subapriya, Ms. N. Radhika proposes a new and efficient framework for the detection and prevention of Distributed Network Intrusions [12]. Since Distributed Denial of Service is caused due to the huge amount of packets flow in the network at the same time. The methodology implemented here is a hybrid combinatorial method of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) using Hashed based pattern matching algorithm and hybrid of anomaly detection and signature based detection.

J. Rameshbabu, B. Sam Balaji, R. Wesley Daniel, K. Malathi introduced a DDoS attack prevention system in Cloud using NEIF based technique [13].

CONCLUSION

The various detection and prevention techniques implemented for the DDoS Attack are analyzed and discussed and hence, by analyzing the various issues detected in the existing methodologies, an efficient framework can be implemented for the improvement of low false alarm rate as well as providing better true positive rate for the detection, classification and prevention of DDoS attacks in the cloud computing system.

Abbreviations

- DoS : Denial of Service
- DDoS : Distributed Denial of Service
- GICTF : Global Inter-Cloud Technology Forum
- SIIF : Standard for InterCloud Interoperability and Federation
- ICF : InterCloud Fabric
- QoS : Quality of Services
- DNS : Domain Name System
- ARP : Address Resolution Protocol
- RIP : Routing Information Protocol
- IP : Internet Protocol
- NIDS : Network Intrusion Detection System
- SaaS : Software-as-a-Service
- PaaS : Platform-as-a-Service
- IaaS : Infrastructure-as-a-Service
- CPU : Central Processing Unit
- DaaS : Desktop-as-a-Service
- CaaS : Communications-as-a-Service
- HaaS : Hardware-as-a-Service
- TCP/IP : Transmission Control Protocol / Internet Protocol
- SYN : Synchronize
- ICMP : Internet Control Message Protocol
- IT : Information Technology
- ABM : Adaptive Bandwidth Management
- IDS : Intrusion Detection System
- IPS : Intrusion Prevention System
- NEIF : Network Egress and Ingress Filtering

ACKNOWLEDGEMENT

Ms. Dalima Parwani carried out the survey on DDoS attacks in cloud framework and drafted the manuscript. Dr. Amit Dutta and Dr. Piyush Kumar Shukla substantially contributed to the conception of

the study, provided considerable inputs into drafting and revising the manuscript. All the authors read and approved the final manuscript.

REFERENCES

1. Kashif Munir and Sellapan Palaniappan "Security Threats/Attacks Present in Cloud Environment", *IJCSNS International Journal of Computer Science and Network Security,* **12**(12): pp. 107 – 114, December 2012.
2. Mohd Nazri Ismail, Abdulaziz Aborujilah, Shahrulniza Musa, AAmir Shahzad, "Detecting Flooding based DoS Attack in Cloud Computing Environment using Covariance Matrix Approach" 2013.
3. Kyung Choi, Xinyi Chen, Shi Li, Mihui Kim, Kijoon Chae, and JungChan Na "Intrusion Detection of NSM Based DoS Attacks Using Data Mining in Smart Grid", *OPEN ACCESS Energies,* **5**: pp. 4091-4109, 2012.
4. Peng Tao, Leckie Christopher, and Ramamohanarao Kotagiri, April 2007. Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys (CSUR),* **39**(1):1–42 ISSN 0360-0300
5. Baldev Singh, Dr. S.N. Panda, Dr. G.S. Samra," Threshold based Approach to Detect DDoS Attacks in Cloud", *International Journal of Innovative Research in Information Security (IJIRIS),* **3**(2): March 2015.
6. Dr. S. SaravanaKumar, R. SenthilKumar, R. Arun Prasad, S. Thiraviam, J. Vignesh," Detecting and Preventing DDoS Attacks in Cloud", *International Journal of Innovative Research in Computer and Communication Engineering,* **3**(3), March 2015.
7. Krishna Modi, Prof. Abdul Quadir Md.," Detection and Prevention of DDoS Attacks on the cloud using Double-TCP Mechanism and HMM-based architecture", *International Journal of Cloud Computing and Services Science,* **3**(2), April 2014.
8. Christian Esposito, Massimo Ficco, Francesco Palmieri, Aniello Castiglione," Interconnecting Federated Clouds by using Publish-Subscribe Service", Cluster Compu., Springer 2013.
9. Amit Khajuria, Roshan Srivastava," Analysis of the DDoS Defense Strategies in Cloud Computing", *International Journal of Enhanced Research in Management & Computer Applications",* **2**(2), Feb 2013.
10. Patel Ankita and Fenil Khatiwala," Survey on DDoS Attack Detection and Prevention in Cloud", International Journal of Engineering technology, *Management and Applied Sciences,* **3**(2): February 2015.
11. G. Preetha, B.S. Kiruthika Devi, S. Mercy Shalinie," Autonomous Agent for DDoS Attack Detection and Defense in an Experimental Testbed", *International Journal of Fuzzy Systems,* **16**(4), December 2014.
12. S. Subapriya, Ms. N. Radhika," DNIDPS: Distributed Network Intrusion Detection and Prevention System", *IJISET- International Journal of Innovative science, Engineering & Technology,* **1**(7), September 2014.
13. J. Rameshbabu, B. Sam Balaji, R. Wesley Daniel, K. Malathi," A Prevention of DDoS Attack in Cloud using NEIF Techniques", *International Journal of Scientific & Research Publications,* **4**(4): April 2014.
14. Rajkumar Buyya, Rajiv Ranjan and Rodrigo N. Calheiros," InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services", Springer 2010.
15. Debajyoti Mukhopadhyay, Byung-Jun Oh, Sang-Heon Shim, Young-Chon Kim, " A Study on Recent Approaches in Handling DDoS Attacks", Cornell University Library, 2010.
16. Toma´s Jirsk, Martin Husak, Pavel Celeda, Zdenek Eichler, "Cloud-based Security Research Testbed: A DDoS Use Case", IEEE, 2014.
17. David Mankins, Rajesh Krishnan, Ceilyn Boyd, John Zao, Michael Frentz, "Mitigating Distributed Denial of Service Attacks with Dynamic Resource Pricing", IEEE 2001.
18. Farzad Sabahi "Cloud Computing Security Threats and Responses", IEEE 3rd

International Conference on Communication Software and Networks (ICCSN), pp. 1-5, 2011.

19. S. Roschke, et al., "Intrusion Detection in the Cloud," presented at the Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Chengdu, China, 2009.
20. N. Mead, et ai, "Security quality requirements engineering (SQUARE) methodology" Technical report of Carnegie Mellon Software Engineering Institute, 2005.
21. J. W.Rittinghouse and J. F.Ransome Cloud Computing: Implementation, Management, and Security Taylor and Francis Group, LLC,CRC Publication, 2010.
22. Ramgovind S, Eloff MM, Smith E. The Management of Security in Cloud Computing, IEEE 2010.
23. Bodkins J, 2008, 'Gartner: Seven cloud-computing security risks', InfoWorlds, viewed 13 March 2009.
24. Stefan Birrer," A Comparison of Resilient Overlay Multicast Approaches", IEEE 2007.
25. Miguel Castro, Peter Druschel, Anne-Marie Kermarrec and Antony Rowstron," SCRIBE: A large-scale and decentralized application-level multicast infrastructure", IEEE 2002.