A Novel Approach to Data Filtration against Packet Flooded Attacks in Cloud Service

Mandeep kaur
Assistant Professor, CEC, Landran, Mohali, India.

Reecha Sood
Assistant Professor, Chandigarh Group of Colleges, Landran, Mohali, India.

Shelly Garg
Assistant Professor, Chandigarh Group of Colleges, Landran, Mohali, India.

Pankaj Palta
Assistant Professor, CEC, Landran, Mohali, India.

Abstract – The term cloud computing seems to originate from computer network diagrams that represent the internet as a cloud. While cloud computing services have numerous potential benefits, there are also potentially significant privacy and security considerations that should be accounted for before collecting, processing, sharing, or storing institutional or personal data in the cloud. In this paper we have discussed clod computing layers architecture and security issues.The usage of remote servers network on the Internet to process data, store and manage, instead of using a local server or any computer" is called cloud computing. Cloud computing is that which totally based on resource sharing rather than any other device to handle applications. Today cloud computing is facing numerous challenges and one of those is Attack on the cloud environment. There are many types of hazardous attack on cloud, as the attack is always in wait for some important data or resource. The most common and most affective attack is Packet Flooding attack and there are many faces of packet flooding. EDoS Attack one of the most commonly and strong packet flood attack on the cloud to make the resources almost inaccessible to the user by flooding the unnecessary packet to the network or site more that its capacity. This paper deals with the analysis of EDoS, DDoS Attacks and Counter measures for these attacks.

Index Terms – DDoS, EDoS attack, Internet Service Provider (ISP).

1. INTRODUCTION

The cloud computing is defined as a collection of software, hardware, storage, networks, services and interfaces that combines to deliver aspects of the services to the user. Cloud computing is one of the most attractive research fields because of its ability to decrease costs coupled with computing while having great potential for growing scalability and flexibility for computing services [3]. Resources like software, hardw are and any information are provided to computers and other devices on demand. It allows user to do those things they want to do buying and building an IT infrastructure or to understand the basic technology [14]. The SLA agreement signed or negotiated between the consumer and service providers so that user will pay only those resources which and how much they used, this phenomena is termed as "pay as per use". With the increase of the widespread of this technology many notorious mind are also there, which want to use cloud resources for their own profits. So security on the cloud is becoming one of the major issues. Attack is one of the concerns of the security issues. There are many types of attack through which data can be hacked or damaged, but here this paper deals with most incidental attack that is EDoS attack. EDoS is basically derived from DDoS attack, which is advance version of the DoS attack. DDoS focus on websites and host applications, target them by absorbing their bandwidth which leads to create disturbance for resource accessibility to legitimate users [19]. These types of attack may halt the business operations and further results to the loss in revenue .this referred to EDoS (Economic Denial of sustainability)[8].

1.1 DDoS attacks

A denial-of-service (DoS) attack is an attempt to make a computer resource (e.g. the network bandwidth, CPU time, etc.) unavailable to its intended users. To overload the necessary network and CPU resources, attackers tend to use a large number of machines to launch the Distributed DoS (DDoS) attacks

Fig. 1 shows the DDoS attack, the cloud represents the internet service provider (ISP), these ISP acts as source of the services from the cloud. For the cloud computing there are two major components one Service Provider and other is consumer. There is agreement called Service Level Agreement (SLA) [7] signed between ISP and users' so that user would be paid as per their usage. But to take profit

from these services the attacker misuses for their own benefits by making loss or damage to others.

DDos attack is very power pack attack to hinder the services, which further causes economical loss. Attackers send numerous requests to the ISP which create bottleneck condition at providers' side [20][11]. As the network is loaded more than its threshold capacity, which makes the resources unreachable to the legitimated user and affect all other packet sharing that path [16][7].

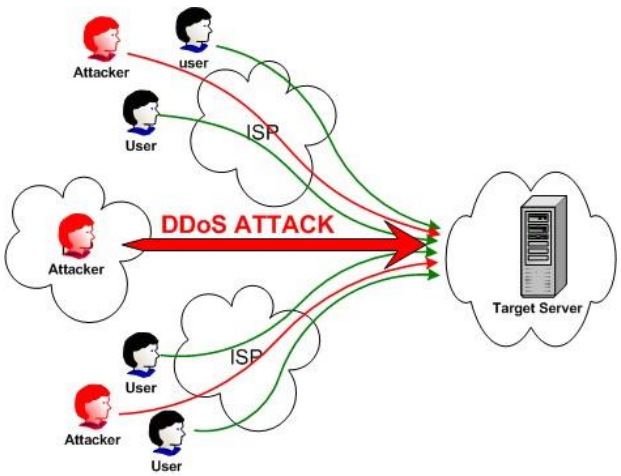

Fig.1 DDos attack

1.2 EDoS attack

DoS is different from traditional DDoS in that, the intention of the latter is to consume all the resources (like memory, bandwidth, CPU etc) of the Web Server thus making it unavailable to its legitimate users. EDoS on the other hand is caused by malicious users who are not interested in following the regular workflow of an E-commerce application by purchasing items but by employing it for their own purposes of entertainment, price-checks and idle surfing. We have a twofold solution, (i) admission control and (ii) congestion control. In the first, we limit number of clients that can simultaneously send requests, thus allowing only enough clients that can be served easily within available resources on the Web server. In the second, we change the priority of allowed clients based on the type of resources they visit and type of activities they perform, thus making the maximum resources available to good clients. We have integrated and evaluated this solution in a Web Application Firewall and found it quite effective in term of resources distribution among clients ranging from good and bad clients.

EDoS-Shield is a mechanism to protect the cloud from the EDoS attack. This architecture consists of two components they are virtual firewall and the cloud verifier node. The virtual firewall acts as a filter. The VF uses the whitelist and Blacklist for making decision. The V nodes use the graphic Turing tests such as CAPTCHA to verify legitimate requests at the application.

1.3 Internet Service Provider

Established and deployed by ISPs, the Internet's largest backbone networks are strategically interconnected by core routers that connect the world's multinational networks. As shown in Figure 2, an ISP network interconnects to other ISP networks and various organizations

The concept of the Internet was based on a decentralized provisioning and management model. ISPs can freely deploy, operate, and manage their networks in addition to selecting partner ISPs for interconnection. No centralized entity comprehensively governs the Internet, although bodies like the Internet Corporation for Assigned Names and Numbers (ICANN) supervise and coordinate Internet communications. The Internet's topology has become a dynamic and complex aggregate of ISPs that are highly interconnected via its core protocols. Smaller branches extend from these major nodes of interconnection, branching outwards through smaller networks until eventually reaching every Internet-enabled electronic device.

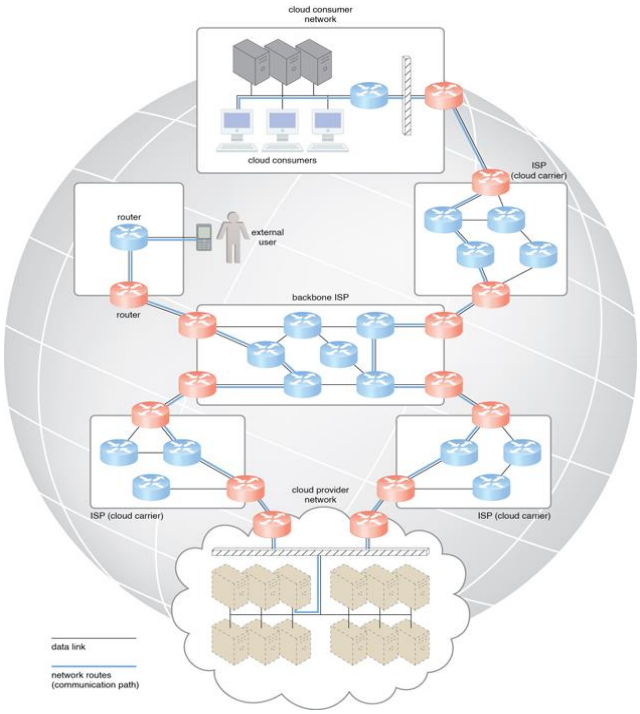

Fig 2 Messages travel over dynamic network routes in this ISP internetworking configuration

2. COUNTER MEASURES FOR ATTACKS

We must know the security requirements or security objective for the cloud. It is important that the security mechanism should satisfy the security requirements.

According to DimitriosZissis,Lekkas, the security objectives within a distributed system are essentially[8]:

To ensure the availability of information communicated between or held within participating systems;

To maintain the integrity of information communicated between or held within participating systems, i.e. preventing the loss or modification of information due to unauthorized access, component failure or other errors;

To authenticate the identity of communicating partners (peer entities) and where necessary (e.g. for banking purposes) to ensure non-repudiation of data origin and delivery;

To ensure the confidentiality of information held on participating systems.

Clear separation of data and processes on the virtual level of the cloud, ensuring zero data leakage between different applications.

To maintain the same level of security when adding or removing resources on the physical level.

There are many mechanisms which serve as a counter to the attacks which disturb security objectives of Cloud. Some few security mechanisms used in cloud such as Intrusion detection system, Packet Filtering, Virtual machine monitoring, trust and on demand mitigation

2.1 Intrusion detection system

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station. The basic functions of an IDS are gathering and analyzing information from various parts of a computer or a network for the purpose of identifying possible security breaches in the form of attacks from external origins and abuse/misuse from within an organization). To assess the security of an IT or network system, IDS often uses a method called "scanning", or vulnerability assessment. A two-step process may be found in an IDS, one a passive component and the other, active. What takes place in the passive component are inspections of the configuration files, password files (to detect weak passwords), and policy audit logs (to detect violations) in a system. In the active component, which is network-based, reenactment of known attack methods take place using installed mechanisms and recordings of system responses to attack reenactments are made. From these processes certain data are captured, usually from packets passing through the system, and reported for subsequent analysis. Hopefully, appropriate steps to counter one or more discovered threats can be taken based on the results of IDS output analyes.

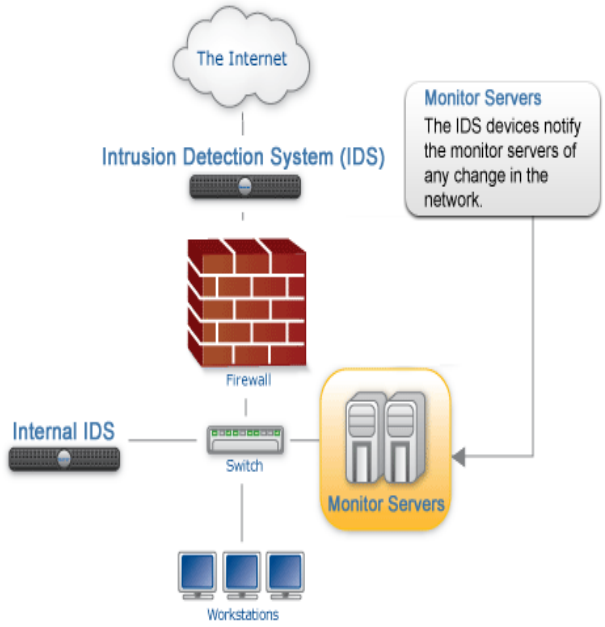

Fig 3. Intrusion dtetection system

2.2 Packet Filtering

Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports. Packet filtering checks source and destination IP addresses. If both IP addresses match, the packet is considered secure and verified. Because the sender may use different applications and programs, packet filtering also checks source and destination protocols, such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). Packet filters also verify source and destination port addresses

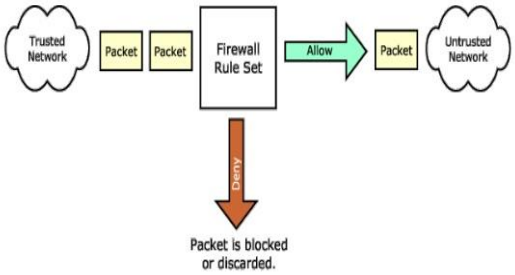

Fig 4. Packet Filtering

2.3 Virtual machine monitoring

A hypervisor or virtual machine monitor (VMM) is a piece of computer software, firmware or hardware that creates and runs virtual machines. A computer on which a hypervisor is running one or more virtual machines is defined as a host machine

2.4 Trust and on demand mitigation

The key barrier to widespread uptake of cloud computing is the lack of trust in clouds by potential customers. While preventive controls for security and privacy are actively researched, there is still little focus on detective controls related to cloud accountability and audit ability. The complexity resulting from large-scale virtualization and data distribution carried out in current clouds has revealed an urgent research agenda for cloud accountability, as has the shift in focus of customer concerns from servers to data. Trust and on demand mitigation means that to trust the firewall and provide solution when needed.

3. RELATED WORK

M. Naresh Kumar et.all[8] described that EDoS mitigation technique is proposed by using In-cloud Scrubber Service in a cloud environment. The key function this scheme is to generate the puzzle to check the authentication of the user. In this paper there are two modes first is normal and second is suspect mode. The In cloud scrubber service is used during the suspected mode. The incoming packets are send to the scrubber service to verify the packets. As per verification is done by scrubber the burden on service provider can triumph.

M.H. Squalli et.all [9] described that EdoS shield technique is used to mitigate EDoS attack. EDoS is Two step mitigation technique against EDoS attack in a cloud computing. Through this machine verification is done in the presence human. The two-step includes Virtual Firewall and verifier Node. The firewall is used to filter out unwanted packets differentiated by white and black list and verifier node is used to verify incoming request by using Turing test. But the proposal has short come in the case of IP spoofing.

S. Vivian Sandar and Sudhir Shenai [13] described a new approach for the attack is shown. This paper proposes an approach for ensuring that EDoS attack based on XML and HTTP do not trigger the auto scaling feature of cloud. This paper mainly deals with the study of DDoS attack through protocols. The cloud services is hosted by Amazon EC2, during attack services are scaled by consuming more Amazon resources which leads to Economic Denial of Sustainability.

Lanjuan Yang et.all [6] perposed a mechanism is proposed for the identification of performer of DDoS attack against cloud. The mechanism used is traceback, filtering techniques to ensure that only relevant or legitimate packets gone through the cloud virtual resource. Until the server's capacity do not exceeds the bumpy packets are also served. In [10] survey is made on types of DDoS attack and their defend methods with IP spoofing. Different ways of DDoS attack is reviewed and for that particular best defend method is discusses. Each method has specific features that makes it more suitable than any other in particular situation.

Gehana Booth et.all [5] presents a classification on cloud computing. Many threats models and specific attack mechanism is discussed. And proposed defend mechanism to counter the attack models. Also highlight the major threats in the cloud instead of having plenty of security mechanism.

A.M. Lonea et.all [2] focuses on detecting and analyses of the Distributed Denial of Service (DDoS) attacks in cloud computing environments. Here solution is proposed for the attack by using intrusion Detection System that is to combine the evidences which are obtained by using Intrusion Detection Systems (IDSs) deployed in virtual machines (VMs) of the cloud systems with data fusion methodologies.

S. K. Parsha et.all [15]proposes the implementing of data access security in cloud network by using the Hierarchical Identity Based Encryption (HIBE). Implementation based on restricting the data access among the unfaithful users that can be attained by introducing the users in hierarchical manner. The data access security is been achieved by uncovering or baring the data only to the trusted and faithful users.

A. Belenky et.all[1] proposed a approach that is scalable, simple to implement, and introduces no bandwidth and practically no processing overhead on the network equipment. It is capable of tracing thousands of simultaneous attackers during DDoS attack. All of the processing is done at the victim. The traceback process can be performed post-mortem, which allows for tracing the attacks that may not have been noticed initially. The involvement of the Internet service providers (ISP) is very limited, and changes to the infrastructure and operation required to deploy DPM are minimal. DPM performs the traceback without revealing the internal topology of the provider's network, which is a desirable quality of a traceback scheme.

4. CONCLUSION

A denial-of-service (DoS) attack is an attempt to make a computer resource (e.g. the network bandwidth, CPU time, etc.) unavailable to its intended users. And EDoS (Economic Denial of sustainability) attack may halt the business operations and further results to the loss in revenue. After the study we have concluded there should be a counter measures for detecting and preventing the EDoS and DDoS attacks. Many authors gave their best counter measures as explained in related work but then also we are not able to prevent from EDoS and DDoS attacks. So to detect and prevent from EDoS and DDoS attacks there should be a counter measure.

REFERENCES

[1] Belenky and N. Ansari, "Tracing Multiple Attackers with Deterministic Packet Marking (DPM)," *IEEE Pacific Rim Conference*

on Communications, Computers and Signal Processing, 2003, pp.49-52.

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

[3] Ayesha Malik, Muhammad Mohsin Nazir "Security Framework for Cloud Computing Environment," A ReviewJournal of Emerging Trends in Computing and Information Sciences vol. 3, No. 3, March 2012.

[4] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," Computer Networks: the Int. J. Computer and Telecommunications Networking, Vol. 44, No. 5, April 2004, pp. 643–666.

[5] Gehana Booth, Andrew Soknacki, and Anil Somayaji, "Cloud Security:Attack and Current Defence", *8th Annual symposium on information Assurance(ASIA'13),* June 4- 5,2013, Albay, NY.

[6] Lanjuan Yang, Tao Zhang. Jinyu Song, Jinshuang Wang and Ping Chen, "Defence of DDoS attack for cloud computing", *In Computer Science and Automation engineering, 2012 IEEE International Conference* on volume 2, pages 626-629, 2012.

[7] Linlin Wu and Rajkumar Buyya, "Service Level Agreement (SLA) in Utility Computing Systems," *Technical Report, CLOUDS-TR-2010-5, Cloud Computing and Distributed Systems Laboratory,* The University of Melbourne, Australia, September 3, 2010.

[8] M. Naresh Kumar, P. Sujatha, V. Kalba, R. Nagori, A.K. Katukojwala, and M. Kumar, "mitigating Economic Denial of sustainibilty on cloud computing using In- Cloud Scrubber service," *In proc. of the 4th International Conference on Computational Intelligence and Communication Network(CICN),*2012.

[9] M.H. Squalli, F. Al-Haidari, and K. Salah, "EDoS shield: a two steps mitigation technique against EDoS Attack in cloud computing," *In Utility and cloud computing(UCC),2011 Fourth IEEE International Conference on,* page 49-56, 2011.

[10] Nisha H. Bhahaduri, "Survey on DDoS Attack and its detection and defence approaches", *International Journal of science and modern engineering* ISSN:23196386, volume 1, Feb 2013.

[11] P. A. R. Kumar and S. Selvakumar, "Distributed Denial- of-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Traceback Mechanisms," in Advance Computing Conference, 2009. IACC 2009. IEEE International, 2009, pp. 1275-1280.

[12] Rajkumar Buyya , Rajiv Ranjan and Rodrigo N. Calheiros "Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities," *Grid Computing and Distributed Systems (GRIDS) Laboratory Department of Computer Science and Software Engineering* The University of Melbourne, Australia.

[13] S. Vivian Sandar and Sudhir Shenai, "Economic denial of Sustainability using Http and Xml", *International Journal of Computer Applications,* 2012.

[14] R.Punitha , D. Vijaybabu, " Data storage security in cloud by using jar files and hierarchal id based cryptography", *ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* Volume 2, Issue 1, January 2013.

[15] S. K. Parsha, M. K. Pasha, "Enhancing Data Access Security in Cloud Computing using Hierarchical Identity Based Encryption (HIBE)," *International Journal of Scientific & Engineering Research* vol. 3, Issue 5, May- 2012, ISSN 2229-5518.

[16] Stephen M. Specht and Ruby B. Lee, "Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures," *Proceedings of 7th International Conference on parallel and Distributed computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems,* pp.543-550.

[17] S. Mukkamala, A.H. Sung,"Detecting denial of service attacks using support vector machines," *Proceedings of IEEE International Conference on Fuzzy Systems,* 2003.

[18] V.Praveena and N. Kiruthika "New Mitigating Technique to Overcome DDOS Attack," World Academy of Science, Engineering and Technology 45 2008, pp. 442-447.

[19] Upma Goyal, Gayatri Bhatti and Sandeep Mehmi, "A Dual Mechanism for defeating DDoS Attacks in Cloud Computing Model", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 3, March 2013.

[20] Zuber A. Baing, Farid Binbeshr "Controlled virual resource access to mitigate Economic Denial of susrainibility Attack Against cloud infrastructures," International confrerence on cloud computing and big data, 2013.