I.J. Modern Education and Computer Science, **2015, 12, 29-34**
Published Online December 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2015.12.04

A Novel Active Data Filtration for the Cloud based Architecture against Packet Flooding Attacks

Shikha Vashisht
Student, Chandigarh Group of Colleges, Landran, Mohali, India
Email: shikhavashisht5@gmail.com

Mandeep kaur
Assistant Professor, Chandigarh Group of Colleges, Landran, Mohali, India
Email: cgccoe.cse.mk@gmail.com.

***Abstract*—**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 and a mechanism is proposed to mitigate the EDoS by using filtration mechanism. The filtration is done on the basis of secure key Exchange which differentiate legitimate user from attacker. The simulation is done by cloud sim as well as Net-Beans and the performance is analyzed over time and data. Using filter the packet loss and time delay occurs in EDoS attack is much reduced.

***Index Terms*—**Cloud computing, DDoS, EDoS attack, Service Provider (SP).

I. 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, hardware 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]. The given below figure 1 shows the DDoS attack on a cloud environment, which intends turns to EDoS because of the economic loss in the cloud at the end it results to loss of revenue to the users or may be organisation[1][2].

Fig. 1 shows the DDoS attack, the cloud represents the service provider (SP), these SP 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 SP 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 S.P 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].

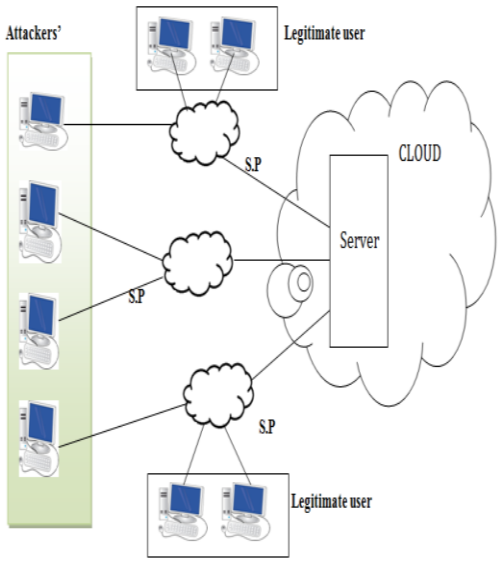

Fig.1. EDoS Attack in a cloud

II. Literature Survey

In this section describes the literature survey for the cloud computing its attack and the mechanisms for the security of the cloud. In [8] 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. In [9] 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 t o 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. In [13] 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.

In [6] 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. In [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. In [2] paper 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. In [15] paper 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.

III. Problem Formulation

Cloud platforms are the emerging network technology and popular for its heavy duty storage and processing facilities. This emerging cloud technology is taking the world into a new age of automatically driven vehicles. This digital medium is prone to hacking and several attacks can take place in the cloud platforms. The DDoS attacks are performed usually by the group of hackers in order to achieve some particular goal. The hackers may aim the DDoS technique to hurt the network dependency and resource availability of some particular online service provider, which may hurt the economic affairs of the particular firm. These attacks are called EDoS attacks or economical denial of sustainability, which specifically affect the popularity of the application specific. These attacks can cause major security issues, accidents, traffic congestion, etc. So, before the initial setup of the cloud application and to run it smoothly over longer time by mitigating these threats in the real-time. In order to mitigate these threats, the attacks must be reviewed thoroughly and the effective solutions should be produced to fill those gaps in cloud platforms. The major attacks on cloud platforms are DoS, Fabrication Attack, Sybil Attack, Selfish driver, Replay Attack, Malicious Attack, etc. All of these attacks cause the unavailability of the resources or can cause the malicious functioning in the cloud applications. DoS (Denial of Service) Attacks are caused by flooding of many packets and result of which is communication hurdle between the cloud nodes or cloud server-client communication. In order to revive and/or retain the performance of the services offered by the service providers and to minimize the economic losses, these attacks have to be checked regularly in the highest possible effective manner.

IV. Proposed Work

In this paper, we are proposing a cloud environment security method to protect the packet flooding attack in the form of EDoS attack, which is a actually a form of DDoS attack launched to gain profits. The proposed model presents the efficient key management scheme to protect against the DDoS attack in order to protect against EDoS which is the cause of economic loss. The economic loss is the main objective of the EDoS attack. The proposed model uses automatic authentication, authorization and accounting model using the secure and fast key sharing mechanism to protect the integrity of the cloud users and their data privacy. As authentication is the main step or first step to implement the security in any network. As authentication help to identify the valid user from a pack of the user which may includes invalid user, attacker or unauthorised user.

A. Experimental Design

The proposed security model will offer and enable comprehensive, trustworthy, user-verifiable, and cost-effective key management for the cloud platforms. The trusted computing base (TCB) will be a node, which will be responsible for the key scheme management. All of the cloud users will communication with the TCBs during the authentication phase, which will ensure the security of further communication with the cloud platform and the end user.

The blue colour palette has been printed in Fig. 2 to define the within limit data. The user who are sending the data in the permitted limit are shown sending the data through the blue ingress point.

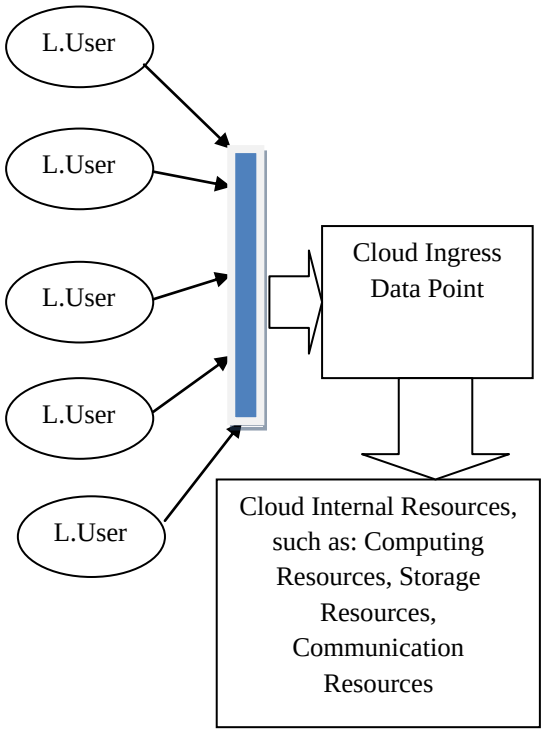

Fig.2. The cloud model with the normal users classified as the legitimate users

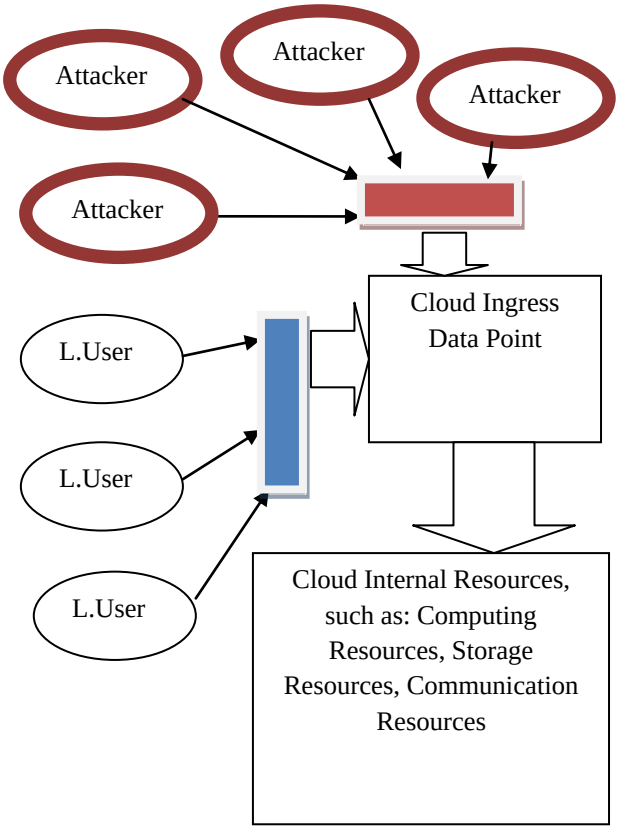

Fig.3. The cloud model has been shown with the legitimate users as well as the attacker nodes.

The blue colour palette has been printed in Fig. 3 to define the within limit data. The user who are sending the data in the permitted limit are shown sending the data through the blue ingress point. The attackers' nodes have been shown sending the data through the red ingress point.

B. Algorithm for Traffic filtration:

1. Start Cloud Environment
2. Start Traffic analyzer program
3. Begin analyzing on incoming traffic
4. Scan every traffic stream separately
5. Set dynamic threshold for incoming traffic
6. If traffic from a source is higher than threshold
   a) filter the traffic amounting over the limit
7. Otherwise
   a) Accept and forward the traffic to the concerned cloud source
8. Repeat step from 4 to 7.

V. Simulator and Simulation Results

The simulation is done by using cloud sim simulator and net beans. The random data is transmitted between server or data centre and user. The analysis is done on the basis of the time and data.

Cloud Sim: Cloud sim is a toolkit for modelling and simulation of multiple Data Centres and associated policies for migration of VMs for reliability and automatic scaling of applications. It provide generalize

and extensible frame work that enable modelling and experimenting cloud computing infrastructure and application services. Cloud Sim provides dynamic insertion of simulation stop and resume. Reason it is used widely is that it is energy efficient management for cloud resource. One more important use of cloud simulator is for optimization of cloud computing [12].

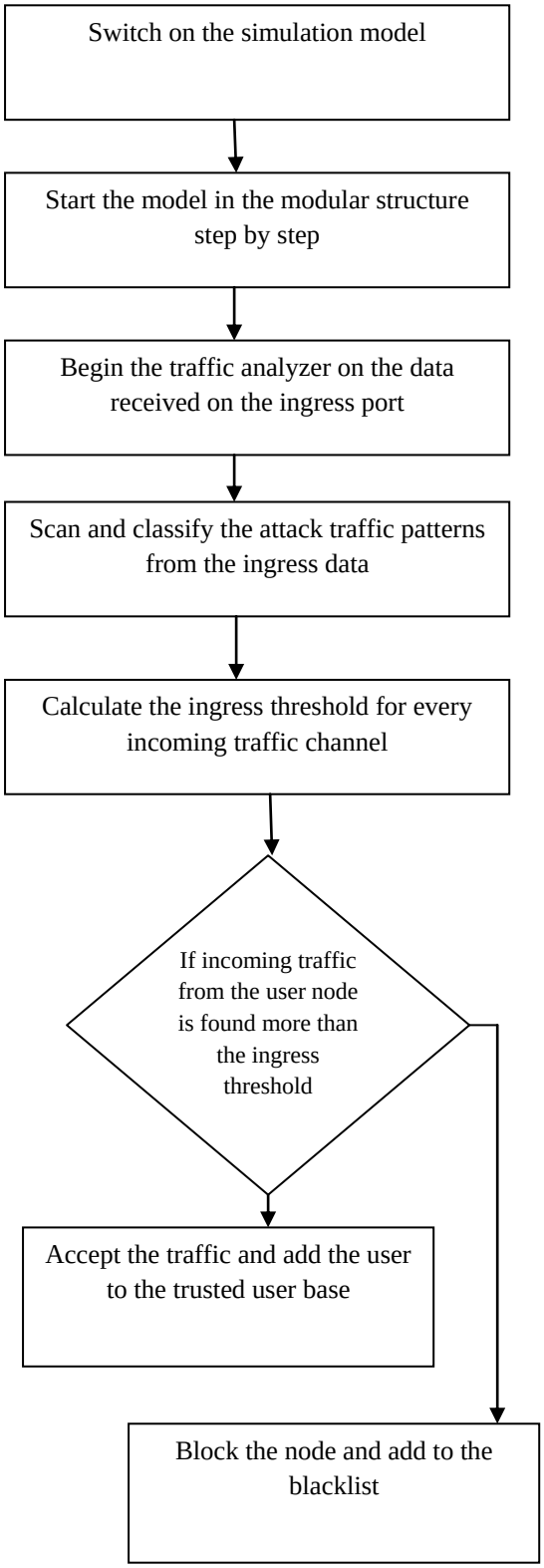

Fig.4. The cloud security model workflow diagram

NetBeans: provides a platform that allows applications to developed from modules that is a set of modular software components. Usage of net beans as given below:

- As a User interface management
- User settings management
- Storage management
- Window management
- As a framework
- Support Visual Library
- Integrated development tools

An EDoS attack is launched to study the behaviour and to prevent the loss occurred by attack, we proposes a security mechanism which is based on the Secure Key Exchange between Service Providers and legitimated user. In this mechanism, it filters out the unwanted traffic coming from the invalid users (Attacker). The valid and invalid user is confirmed with the key Exchange, those user who have same key table as SP have are legitimate user and those don't have are invalid users. The system designs such that it contains three cases as shown below:

1. Normal
2. With Attack
3. With security

The normal case is considered as the network without any attack or any other interruptions in network. The second one is With Attack case which describes the interruption of the intruder in the network by launching different attacks specially consider EDoS attack here. The third case is implementing the proposed security model.

The following are the parameter through which the analysis is done

Submission time: Time taken to complete overall task. The submission time is the parameter which indicates the total time for the completion of the processes under the given cloudlet.

Finish time: Time taken to create particular instance. The finish time is the final time taken by the processes taken for the completion of all of the processes of a given application or application task running under different cloudlets.

Data: Packet that is transmitted to network. This parameter indicates the total volume of data transferred between the two nodes

Packet loss: Packet drop or lost due to congestions. The parameter indicates the number or ratio of the lost packets during the data transmissions on the given communication link.

In Table 1 with first run of the simulation, random data is transmitted. During attack the time delay is increased, which is shown by both finish and submission time that is 12500 and 5500 and packet loss is 1870.

But when the next time simulation is run, the random data is transmitted and DDoS attack is also there but we

implement a security filter, which filter out unnecessary packets. With end of simulation the time overhead is lesser as well as there is decrease in packet loss as compare to Attack case.

Table 1. Time based analysis of the proposed model in comparison with attack situation and normal situation on first rotation 1

Case	Data	Submission time	Finish time	Packet loss
Normal	10000	4700	615	0
With Attack	12500	5500	3800	1870
With Security	13777	4800	2500	689

Similarly Table 2, 3 and 4 shows the results of the simulation every time when it is run. To get the better results we take more and more results so that more accurate results we get.

Table 2. Time based analysis of the proposed model in comparison with attack situation and normal situation on second rotation 2

Case	Data	Submission time	Finish time	Packet loss
Normal	12000	4700	620	0
With Attack	13000	5500	3850	1875
With Security	12500	5000	1700	800

The Table 2 shows the packet loss during the attack is 1875 and the packet loss after implementing security model is 800. There is a huge decrease in the packet loss with the security model, which is about 1075.

Similarly for the time parameters (submission and finish time) the submission time is 5500 with attack and 5000 with security, there is benefit of 500. And in finish time the value is 3850 with attack and it decreases to 1700 with security implanted.

Table 3. Time based analysis of the proposed model in comparison with attack situation and normal situation on third rotation 3

Case	Data	Submission time	Finish time	Packet loss
Normal	10000	4750	620	0
With Attack	1400	4750	3880	1875
With Security	1421	5300	1710	713

Table 4. Time based analysis of the proposed model in comparison with attack situation and normal situation on fourth rotation

Case	Data	Submission time	Finish time	Packet loss
Normal	10000	4700	620	0
With Attack	13965	5500	3850	2095
With Security	11983	5000	1700	599

Final results are based on the comparison of the time and packet loss of the attack case and security case. In normal case we consider packet loss is zero for every time we run the simulation. After implementation of the security filter the packet loss is much lesser than the attack. And time required by the data over the network is also reduced through security.

Table 5. Average Time based analysis of the proposed model in comparison with attack situation and normal situation

Case	Data	Submission time	Finish time	Packet loss
Normal	10500	4712.5	616.25	0
With Attack	13366.25	5525	3843.75	1929
With Security	13120.25	5025	1902.5	700

We had run the simulation for four times to get unambiguous and meticulous values with respect to time and packet loss. Table 5 is the resultant of all the simulation results which represents the average result of all the above simulation. It gives the average value to estimate the better outcome. Final average result shows the packet loss after security is 700 approx. and without any security during attack loss is 1929. The difference is about 1229 packets. There is also a big difference in the time during attack and with security as shown in the table.

VI. Conclusion

With the phenomenon and worldwide use of the cloud computing, it has not only attained the attraction of the user but also focuses the attention of the attackers. The EDoS attacks more targets on cloud services. As these types of attack more pivot on economy and related things. The main motive of these attacks is to make economic loss of others or to get their own profits. To overcome these problems we proposed a secure key Exchange mechanism, which help to filter out the unnecessary packet coming from unauthenticated user. Above results shows the how the proposed mechanism helps to overcome from the time as well data overhead and packet loss. The overall submission time improves by 9% from attack (submission time) and finish time by 50.5%. As shown on the table 5 the average packet loss during attack is 1929 and the average packet loss with implementing security is 700 packets. So there is a big decrease in the loss which is nearly 1229 packets. The packet loss is improved by 63.7% from attack case.

References

[1] A. 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.

Authors' Profiles

Er. Shikha Vashisht Born on 13, March, 1991. She has completed B.tech (Information Technology) from GreenHills Engg. College(H.P.U), Solan, India in the year 2012. She is pursuing M.tech (Computer Science) from CGC College of Engineering, Landran, Mohali, India.

Er. Mandeep Kaur working as a Astt. Prof. at Chandigarh Group of Colleges, Landran in CSE Department since July 2011. She has done B.tech from IET Bhaddal in 2009 and M.tech. from CEC, Landran 2011. She had published 3 International and 4 National research papers