CREDIT BASED METHODOLOGY TO DETECT AND DISCRIMINATE DDoS ATTACK FROM FLASH CROWD IN A CLOUD COMPUTING ENVIRONMENT

N.Jeyanthi, Hena Shabeeb and Mogankumar P.C.

School of Information Technology and Engineering
VIT University, Vellore – 632 014, Tamilnadu, India

ABSTRACT

The latest trend in the field of computing is the migration of organizations and offloading the tasks to cloud. The security concerns hinder the widespread acceptance of cloud. Of various, the DDoS in cloud is found to be the most dangerous. Various approaches are there to defend DDoS in cloud, but have lots of pitfalls. This paper proposes a new reputation-based framework for mitigating the DDoS in cloud by classifying the users into three categories as well-reputed, reputed and ill-reputed based on credits. The fact that attack is fired by malicious programs installed by the attackers in the compromised systems and they exhibit similar characteristics used for discriminating the DDoS traffic from flash crowds. Credits of clients who show signs of similarity are decremented. This reduces the computational and storage overhead. This proposed method is expected to take the edge off DDoS in a cloud environment and ensures full security to cloud resources. CloudSim simulation results also proved that the deployment of this approach improved the resource utilization with reduced cost.

KEYWORDS

Cloud, DDoS attack, Flash crowds, Reputation-based, credits.

1. INTRODUCTION

Cloud computing is a subscription-based promising technology which provides everything to its dependents as 'service' on demand basis. It extends the IT capabilities with a viable option of computation through Internet. As it is a 'pay-as-u-go' model, the companies are migrating towards cloud at a much faster pace. It has also unchained the users from the burden of resource management and maintenance, which is all done by the Cloud Service Provider (CSP). Users can access the services from anywhere at any time, provided they have any Internet enabled system (which can be desktops, laptops, mobile phones, tablets etc) with any browsing software.

The new paradigm, which is an amalgam of various prior models such as distributive computing, grid computing and utility computing, also encompasses on the techniques like pooling, sharing and virtualization of resources. Metered service (bill on use) and elasticity (scale up and down on demand) are other hallmarks of the new model. The cloud comes up with three deployment models (public, private, and hybrid) and delivery models (Software as a Service [SaaS], Platform as Service [PaaS] and Infrastructure as a Service [IaaS]). The public cloud is open for all whereas the access to a private cloud is restricted to the owners and customers of an organization. The cloud SaaS freed the users/organizations from installing the software they need in their PCs. E.g. CRM software. The PaaS provides the platform such as programming language that is needed by users to develop Apps. The network bandwidth, database storage and all are coming under IaaS.

DOI : 10.5121/ijnsa.2013.5511

Unfortunately, cloud with its rich asset of resources and large number of customers, has obviously engrossed the attackers also. It has to encounter all the security threats that any other Internet enabled service do. The list goes like trustworthiness of the CSP, access control, authentication and identification, availability, policy integration, audit and so on. Among these, the threat against availably, Distributed Denial of Service (DDoS) attacks, which floods the CSP with illegitimate traffic is the most challenging, damaging and significant one. As compared to single-tenant infrastructures, the impact of DDoS on cloud is perilous. Even though cloud has the feature of rapid resource provisioning, the elastic nature of cloud serves the illegitimate traffic also. This may lead to exhaustion of critical resources. Again, the organizations which are reliant on these CSPs may lose millions of dollars due to unavailability of service at correct times. This may even force them to move on to other CSPs which in turn affect the reputation as well as the income of CSPs. Thus, this ill-guarded security threat has to be dealt with soon, so as to make use of cloud benefits to full extend.

Although, various researches are going on in this regard and many solutions exist, there are many pitfalls for them like computational and communicational overhead, high memory consumption, cost, usage of critical cloud resources itself for discriminating the attack traffic etc. Most of the methods allows the attack traffic to arrive at CSP and then only takes actions against mitigation. In this paper, we are proposing a new framework to defend against the intractable attack of DDoS by giving reputation to users according to the credits they attained. The observation that attack traffic exhibits similar flow characteristics is deployed here. The credits of clients who show similarity in traffic flow are decremented and such requests are dropped. The ill-reputed clients without any credits are blacklisted and blocked. Our scheme claims less computational overhead and faster detection of attack. The method treats the well-reputed clients with equal priority and also presents a notification mechanism to aid the well-reputed users get rid of probable viral attacks due to which they send request contributing to DDoS traffic.

Remaining of this paper is organized as follows: Section 2 presents the literature survey. Section 3 gives light to the proposed solution and section 4 concludes the paper.

2. LITERATURE SURVEY

The security concerns of cloud environment are the most widely discussed topic today. Various defense mechanisms exist today for detecting and mitigating the number one threat to cloud computing, DDoS attack. The elastic cloud can't distinguish the attack traffic and legitimate traffic by its own. So, the traffic has to first authenticated and filtered. These include the approaches like passwords, cryptography, puzzles, trust-based, reputation-based etc.

An overlay based crediting mechanism called OverCourt, has been proposed in [3] in which the users are classified as well-behaving and ill-behaving based on their behavior. VIP paths are used for tunneling the requests from well-behaving users and non-VIP path for others. Based on whether a user gets response from server or not, they are classified. The credits are incremented when the user gets a response. This method has the advantage that it is an overlay a based network and needn't have to modify any existing infrastructure. An overcourt gateway and two crediting routers do the task of detecting the malicious traffic and discarding them. A credit decaying mechanism is employed to address the issue of dynamic address allocation. But, the method assumes that the legitimate users will back off during attack period and this is not always the case. The criterion for crediting the users based on response is also not a good deal every time as there are chances that attackers may also get the responses. In [1] the reputation of a flow is found based on the credit acquired due to its diversity in packet size. The attackers usually prefer to send small size packets. The flow having LOW reputation is malicious and those falls in HIGH range of the scale is legitimate. But packet size cannot be considered as a measure of legitimacy.

The fine grained capabilities are used in [2] to grant tickets to clients. The clients request for service is preceded by a ticket request. This request contains the credits and penalty values acquired by clients in previous interactions. But, this method fails if the attacker is human. Also, a user can fool the provider by turning hostile after acquiring the ticket.

Apart from these, the information distance [4], inter arrival time of packets, flow correlation coefficient [5] are various other methods proposed in this regard. The [6] classifies the packets based on their predictability of arrival rates. None of this method can be considered as an infallible means of defense against the threat of DDoS attack.

Comparison among the existing Trust based techniques is presented in Table.1.

3. PROPOSED SOLUTION

The proposed solution classifies the clients as well-reputed, reputed and ill reputed based on the credit values they acquire as a consequence of their behavior. Credit can have value ranging from LVALUE to HVALUE (which can be fixed by CSP). Clients having credit values greater than a prefixed value, PVALUE is categorized as well-reputed clients. The requests from such clients will be tunneled through a special channel, where they can access all critical resources of CSP with equal priority. The clients who has credits values between the LVALUE and PVALUE is treated as reputed and such clients are allowed limited access to CSP resources and they are not tunneled through the special channel. The requests from other clients whose credit value is less than the LVALUE are dropped and such clients are blacklisted as ill-reputed clients, so that they are blocked in future also.

Table 1: Comparison Table on the surviving Trust based techniques

Trust based techniques	**Advantages**	**Disadvantages**	**Simulation/ Experiment work**
Trust Ticket Deployment [5]	Simple method No third party involved in issuing trust ticket Data owner can have control over offloaded data as well as users Trust ticket reduces the interactions between users and CSP Data is encrypted twice, once by data owner, and next by CSP Clear logical sequence of tasks. Data owner can update the expiry time of trust ticket of any user at any time Overall computation time is reduced	Limited for SaaS CSP can insist the users to share the Key. Can't rely on the trust of Online registration process	Java Network Programming-Emulated Cloud Environment using VMware ESXi 4.1 Hypervisor based platform
Service Trustiness and Resource Legitimacy in Cloud Computing [3]	Support for dynamic nature of cloud	Not experimentally proved.	Not proved experimentally
Above the Trust and Security in Cloud Computing: A Notion towards Innovation [4]	Secure channel is established Better than SSL	Trustworthiness of CSP can be questioned KDC should also be a trusted entity Not proven Experimentally	Not proved experimentally
Use Trust Management Module to Achieve	safeguard both the customers and providers cross-cloud environment Improved flexibility and	Trustworthiness of the so-called familiar CSPs	Simulation

Effective Security Mechanisms in Cloud Environment [8]	portability of cloud system. help to increase the interoperability		
A Novel Cloud Bursting Brokerage and Aggregation Algorithm for Multi Cloud Environment [7]	Interconnectivity Security resource sharing mapping	No experimental results.	Not proved experimentally.
Security Agents: A Mobile Agent based Trust Model for Cloud Computing [6]	Mobile agents-load balancing, fault tolerance, network management etc. Attacks on VMs can be prevented Data audit & event logging	Session key management No experimental results	Not proven experimentally.
A Model for User Trust in Cloud Computing [1]	Evaluated various parameters influencing the trust		Online Survey, Likert Scale
A Trust Management Model to enhance security of Cloud Computing Environments [9]	robust, fault tolerant and secure cloud computing detect malicious middle nodes		CloudSim toolkit
Cloud security using FPGA [2]	Can't get user data even if the attacker knows user credentials. Security system at user side	Hardware failure of FPGA Physical access to FPGA vicinity	Not proven experimentally

3.1. Assumption

The attacker will usually instigate DDoS attack by finding vulnerable systems in the network (E.g. having no anti-virus protection) and install dreadful programs in them which can make those systems to send requests to the target upon the command of the attacker. These vulnerable systems (zombies) which are distributed across the network sends request packets of similar pattern to the target as per the instructions in the installed programs. Hence, the attack flow will be almost similar in nature compared to the flash crowd flow coming from legitimate users. This observation is used here to distinguish DDoS attack traffic from flash crowd.

Fig. 1 depicts the flow diagram of the proposed credit based concept. When the CSP receives requests for service from the clients, it is checked whether the resources are getting flooded or not. In normal case, the system will check whether the user who has sent the request is a new user or not. If he is a new user, his credit is set to MVALUE and assigned the default path where he has limited access of CSP's resources. If the user is an already existing one, his credits are incremented. In resource overload period, the flow is analyzed to find the similarity and similar flows are discarded. The credits of senders of such flow are checked. If he is a well-reputed user, he is notified about the likelihood of presence of some harmful programs in his system. If he is ill-reputed user, he is blacklisted and blocked from sending request in future. The clients who contributed to dissimilar flow are considered as legitimate users and their credits are incremented. They may be allowed with restricted or full access to CSP's resources based on their credits. They reach the CSP through the assigned path.

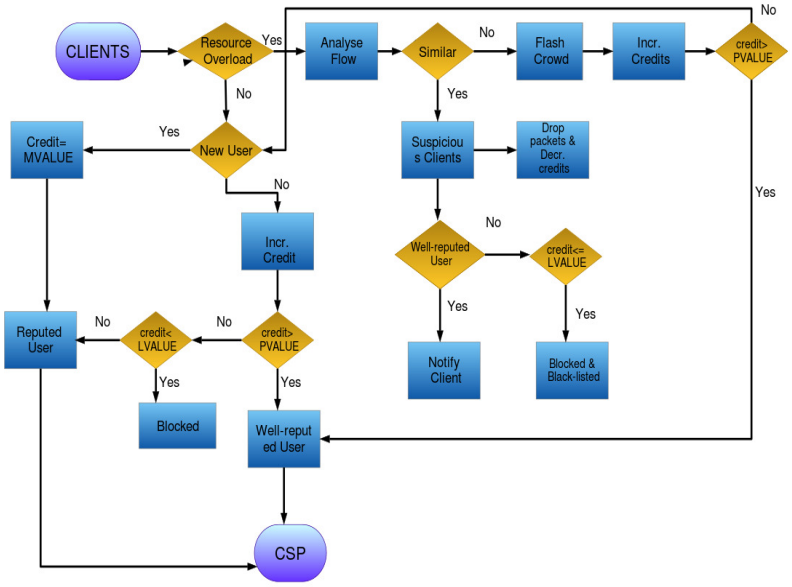

Figure 1. Working model of the credit based system

3.2. Crediting Mechanism

Initially, all clients are assigned a credit value, MVALUE, which is the mean of LVALUE and HVALUE as represented in equation (1),

$$\text{MVALUE} = \frac{\text{LVALUE}+\text{HVALUE}}{2} \quad \textbf{(1)}$$

Under normal circumstances, the credits of all clients are incremented according the following equation:

$$Credit_{new} = \min(incr * Credit_{old}, HVALUE) \quad \textbf{(2)}$$

where is an increment factor that can be fixed randomly by the CSP.

Under attack, the CSP will experience resource overload and the credits of clients who send almost similar request are reduced.The credit values of such clients are decremented according to following equation:

$$Credit_{new} = \max(Credit_{old} - decr * Credit_{old}, LVA \quad \textbf{(3)}$$

where is a decrement factor fixed by the CSP.

If those clients were already in the well-reputed list, they are notified about the chance of a virus or Trojan attack and the decrement in the credit. Thus, they can take necessary actions to come out of viral attack and escape from being penalized further. The credits of other clients are incremented as per eqn. (1). Traffic from such clients is considered to be as flash crowds and is processed for providing the requested service.

A credit expiring mechanism is employed which gradually decrements (until MVALUE) the credit value acquired by a client with time to address the issue of dynamic IP address allocation.

3.3. Credit Based Architecture

As shown in Fig.2, the proposed architecture consists of a forward proxy server, which acts as a gateway between the user's private network and CSP network, a load balancer and a coordinator router. The traffic to datacenters is routed through respective flow routers (R1, R2, R3, R4 & R5), which can analyze the flows' time of receipt, route, and rate of flow. The flow routers will communicate the time of receipt and rate of flow to the coordinator router and coordinator router compares the results it got from all flow routers to distinguish the traffic from attacker and legitimate users.

The requests from the users are received by the proxy server, which finds whether there is any resource overload in the CSP. If there is no resource overload, the proxy server will check whether the requests are coming from new user or not. After assigning the credit MVALUE for new user, their requests will be forwarded to the CSP through default path. For others, credits are incremented and well reputed users' requests are tunneled through special path whereas the reputed users are assigned the default path.

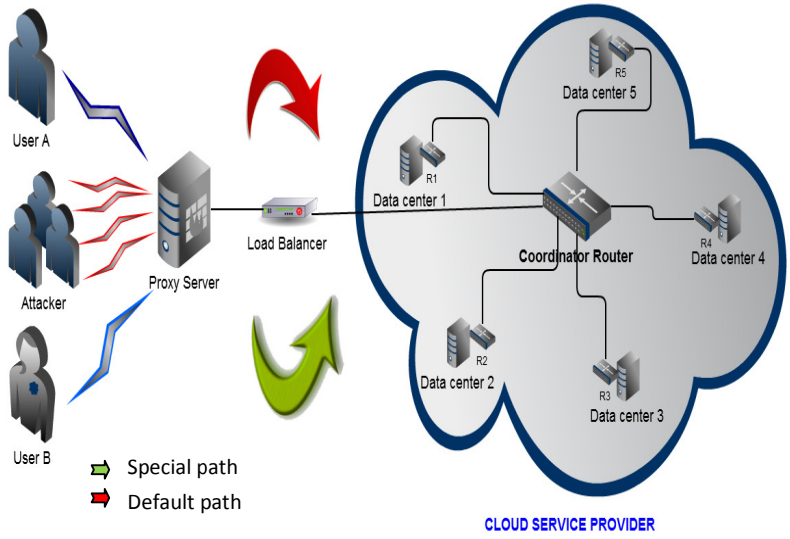

Figure 2. Architecture of Credit based method

When flooding occurs, the proxy server notifies the load balancer and the traffic will be distributed to the to the flow routers which are not busy at that instant. The information regarding the state (busy or not) of flowrouters will be communicated to the load balancer by the coordinator router. Flow router finds time of receipt and flow rate. After discarding the suspicious flow, the coordinator router informs the proxy server about the legitimate clients. The credits of such clients are incremented by the proxy server and their reputation is checked based on which they are assigned path to the datacenters in cloud.

3.3.1. Virtues of Proposed Concept

- The method doesn't have to maintain any predefined profiles of traffic, or history of communication. Only thing that has to store is the credit and corresponding reputation of each client.

- The credit expiry mechanism doesn't allow the credits acquired by one client to be inherited by anyone due to dynamic IP address allocation.

- As flow routers do the function of flow analysis and load balancer distributes the tasks to these routers which are not busy at the instant, there won't be any flooding.
- Notification mechanism to well reputed users about the likelihood of presence of malicious programs.

3.3.2. Performance Analysis

This section presents the comparative analysis of CSP's performance in service delivery before and after implementing our method in the Cloud environment.

Traffic at Datacenter

The traffic at datacenter includes the requests from legitimate users as well as attackers. This will contribute to flooding. Credit based system has completely eliminated the requests from ill-reputed users where as the well- reputed users are given full access as before. As shown in Figure 3, the users 2 & 6 have submitted 500 tasks per second and user 9 & 10 has submitted about 250 tasks per second. The users 3 & 5 have also submitted more than 100 requests per seconds.

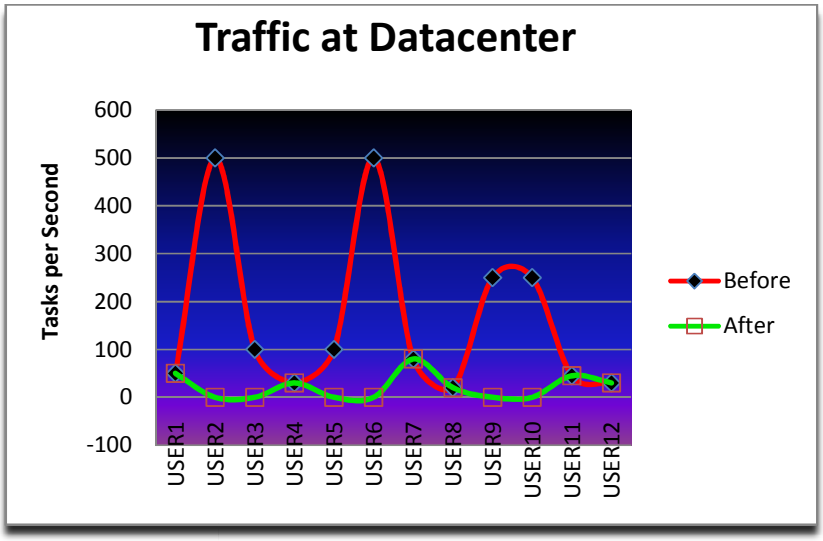

Figure 3. Traffic at Datacenter before and after implementing solution

The increased spike, at the users 2, 6, 9 and 10, denoted that they are attackers and users 3 and 6 are suspicious users. The tasks submitted by these users are completely discarded without disturbing the legitimate clients after employing our method. Thus, credit based method reduced the flooding at CSP and hence CSP can perform more efficiently even in the case of attack period.

Resource Utilization

Resource utilization here means how much percentage of CSP Datacenter resources are allotted to each client. This includes the CPU, RAM and Bandwidth. As per the proposed method only well-reputed users are given full access to CSP resources, reputed users are given limited access and ill reputed users are fully blocked.

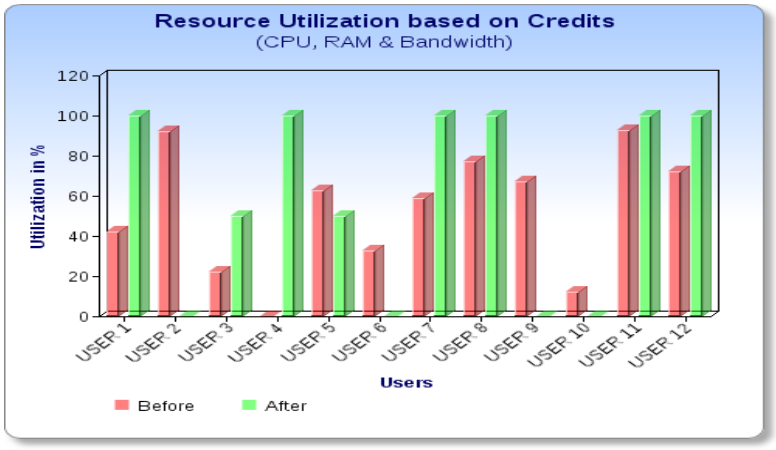

Figure 4. Resource Utilization based on credits

The graph in Figure 4 depicts that well reputed users such as users 1, 4, 7,8,11 & 12 are given full access to CSP resources. The users 3 & 5 who are suspicious are given limited access to resources whereas the users 2, 6, 9 & 10 are completely blocked from accessing the CSP resources. Earlier the users were given random resource allocation due to which well reputed users also faced inefficient service delivery from CSP.

Processing Cost

The processing cost here means the cost incurred at each Datacenter in processing the requests from all users.

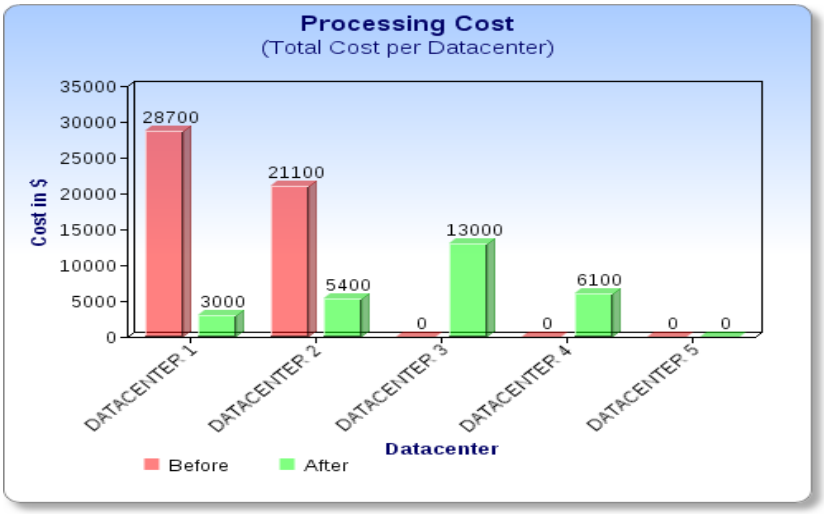

Figure 5. Processing Cost per Datacenter

The processing cost at each datacenter has decreased tremendously after our method has been applied. Instead of giving as much task as possible to one datacenter, the load is distributed among the datacenters which will in turn lessen the response time for serving clients requests. As shown in Figure 5, earlier only Datacenters1 & 2 does all the processing and other DCs were idle. But, after implementing this credit based solution, all datacenters contributed to CSP service delivery and hence helped in enhanced performance and reduced response time.

4. CONCLUSION

Credit based methodology could detect the DDoS attacks and discriminate it from the impatient users i.e. flash crowds. This method could also prevent the environment from future attacks. The experimental results proved the claim. . DDoS attacks are reported to be the number one threat which risks the cloud service providers as well as customers with huge financial and reputation loss. Credit based could achieve better resource utilization with reduction in cost. Hence this method could be cost effective also. Cloud computing which has invaded almost the entire of IT world is facing terrific setbacks due to various security issues prevailing in the cloud environment. This method helps to mitigate the DDoS attack and at the same time processes the flash crowd and provides them with requested service. The method is efficient in terms of computational overhead and memory consumption. The communication between the entities consumes time. Even though, owing to the adeptness of our method to detect and put off the outrage of DDoS in cloud which handles critical business of and provide services to a huge community, the communication overhead which may crop up can be ignored.

REFERENCES

[1] Haiqin Liu, Yan Sun, Victor C. Valgenti, and Min Sik Kim : TrustGuard: A Flow-level Reputation-based DDoS Defense System. In: 5th IEEE Workshop on Personalized Networks, pp.287-289 (2011)

[2] Maitreya Natu, Jelena Mirkovic: Fine-Grained Capabilities for Flooding DDoS Defense Using Client Reputations. In: ACM, pp. 105-112 (2007)

[3] Ping Du, Akihiro Nakao: OverCourt: DDoS Mitigation through Credit-Based Traffic Segregation and Path Migration. In: Computer Communications 33, pp. 2164–2175(2010)

[4] Shui Yu, Theerasak Thapngam, Jianwen Liu, Su Wei and Wanlei Zhou: Discriminating DDoS Flows from Flash Crowds Using Information Distance. In: Third International Conference on Network and System Security, IEEE, pp.351-356 (2009)

[5] Shui Yu, Wanlei Zhou, Weijia Jia, Song Guo, Yong Xiang, and Feilong Tang: Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient. In: IEEE Transactions On Parallel And Distributed Systems,, pp. 1-7 (2012)

[6] Theerasak Thapngam, Shui Yu, Wanlei Zhou and Gleb Beliakov. In: Discriminating DDoS Attack Traffic from Flash Crowd through Packet Arrival Patterns. In: IEEE Conference on Computer Communications Workshops, pp. 952– 957 (2011)

[7] QI Chen, Wenmin Lin, Wanchun Dou, Shui Yu: CBF- a packet filtering method for DDoS attack defence in cloud computing. In: IEEE 9th International conference on Dependable, Autonomic and Secure Computing,427-434, (2011)

[8] Ahmad Rashidi and Naser Movahhedinia: A Model for User Trust in Cloud Computing. In: International Journal on Cloud Computing: Services and Architecture (IJCCSA), vol.2, No. 2 (2012)

[9] Priyank Singh Hada, Ranjita and Mukul Manmohan: Security Agents: A Mobile Agent based Trust Model for Cloud Computing. In: International Journal of Computer Applications, (0975-8887), vol.36 (2011)

[10] Wenjuan Li, Lingdi Ping and Xuezeng Pan: User Trust Management Module to Achieve Effective Security Mechanisms in Cloud Environment. In: ICEIE,Vol. 1 (2010)

[11] Pritesh Jain,Dheeraj rane and Shyam patidar: A Novel Cloud Bursting Brokerage and Aggregation(CBBA) Algorithm for Multi Cloud Environment. In: Second International Conference on Advanced Computing &Communication Technologies (2012)

[12] Xiaodong Sun ,Guiran Chang and Fengyun Li: A Trust Management Model to enhance security of Cloud computing Environment. In: 2nd International Conference on Networking and Distributed Computing (2011)

[13] Mahbub Ahmed and Yang Xiang: Trust Ticket Deployment: A Notion of a Data Owners Trust in Cloud Computing. In: International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11(2011)

[14] N. Jeyanthi and N.Ch.S.N.Iyengar, Packet Resonance Strategy: A Spoof Attack Detection and Prevention Mechanism in Cloud Computing Environment, International Journal of Communication Networks and Information Security, Vol.4,No.3, December 2012, pp.163-173.

[15] Jeyanthi, N.; Vinithra, J.; Sneha, S.; Thandeeswaran, R.; Iyengar, N.Ch.S.N., "A Recurrence Quantification Analytical Approach to Detect DDoS Attacks", IEEE International Conference on Computational Intelligence and Communication Networks (CICN), 2011, pp.58 – 62.