International Journal of Security and Its Applications
Vol. 10, No. 8 (2016), pp.277-294
http://dx.doi.org/10.14257/ijsia.2016.10.8.24

A Review on Distributed Denial of Service (DDoS) Mitigation Techniques in Cloud Computing Environment

Junath Naseer Ahamed and N. Ch. S. N. Iyengar*

Information Technology Department, Ibri College of Technology,Oman
**School of Computer Science and Engg. , VIT University, Vellore -14,T.N ,India*
junath.naseer@ibrict.edu.om , nchsniyr@vit.ac.in

Abstract

Distributed Denial of Service (DDoS) attack becomes a serious hazard for cloud computing environments as they target the victim and completely suppress the Datacenter to serve for its legitimate clients.This work focus on analyzing the several works and suggesting the better approach to suit cloud environment to detect and to maintain better detection accuracy. Also we have made historical comparison of research works of DDoS mitigation schemes with respect to cloud computing environment. The comparison is also made on five existing research works and provided a summary of them which evaluates the detection accuracy of each work.

Keywords*: DoS, DDoS, Cloud Computing, DDoS Mitigation, Flashcrowd.*

1. Introduction

Cloud Computing is a technology which gains all the advantageous features of all its ascendants technologies and stands out as a brimming and optimal solution for the growing IT services. Cloud computing involves characteristics like on-demand service provision, extreme resource virtualization, being elastic and flexible in allocation and release of service provision like storage, network, software applications, servers and its services. Some key advantages of acquiring this most beneficial technology are pay-as-per-use, high fault tolerant, high scalability, improved performance, better and quicker infrastructure setup, least or no infrastructure / platform maintenance. Cloud computing have certain characteristics like Agility, Elasticity, multitenancy, location independency, on-demand service, resource pooling. *Agility, Location and Device Independence, Resource pooling with Multi-tenancy* are some of the distinguishing characteristics that allows many firms to acquire the cloud technology. Multiple business teams can interact within the same cluster of resources who acquires the same resource configuration. Precise authorization helps in identifying different business groups. Once any business groups' resource is released, their resources are pooled to share again with other groups.

The Organization of rest of this paper is Section 2 explains the DDoS, its variants of DDoS and Section 3 draws some illustrative case and after effect of DDoS, section 4 briefs the motivation of this survey, a collection of research significance from various authors. Section % provides a detailed comparison of related articles and finally section 6 concludes the significance this research study by revealing some studies on DDoS mitigation schemes.

* Corresponding Author

ISSN: 1738-9976 IJSIA

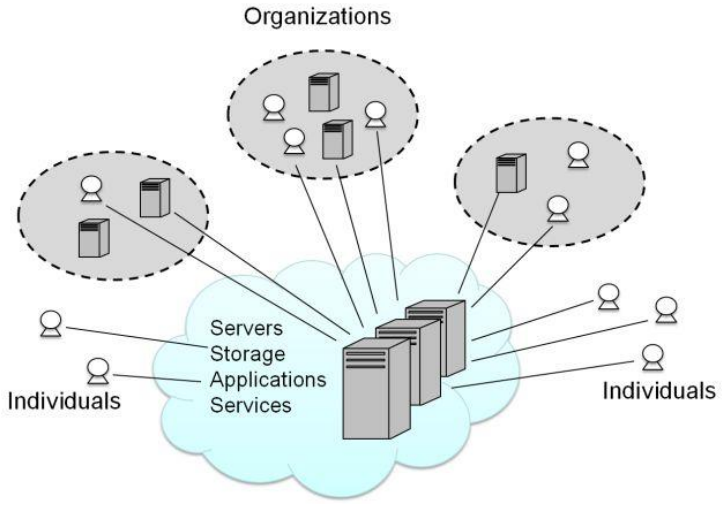


Figure 1. A Typical Cloud Computing Model (As per opengroup.org)

Cloud computing has several of its own feature to serve better but behind its significance, it also has its own misleading security challenges which in not addressed will lead to a serious trouble of being permanently data unavailability. Some of the serious threats at cloud computing are: *Data breach*: In a multitenant environment, a damage or flaw posed by any one of the shared business group, the whole tenants who share such infrastructure would be affected by the data leakage. *Data loss*: A malicious attacker gaining access to the sensitive data could lead to the loss of business and data privacy to the subscribers'. This integrity loss and degraded confidentiality leads to serious data loss. *Denial of service (DoS):* DoS is the highest rank of security threat. DoS has now extended as (Distributed Denial of Service) DDoS which launches the attack for distributed sources to increase the volume of attack and to create a serious damage to the servers, services and the residing sensitive data. DoS and its variants creates temporary or permanent outages which depends on the volume of attack. *Malicious insiders*: An requestor who can be an employee but acting towards destroying his own organization's resource.

2. Unveiling the Presentation of DDoS:

A DDoS (Distributed Denial of Service) is a kind of attack launched by the globally distributed attackersto deplete the available resources which results in server unresponsiveness and service unavailability so that the legitimate users cannot gain access. DDoS is an extensive effect of DoS, the difference is the volume and vulnerability of the attack launched and the number of attacker attempt to attack the server resource. Higher the effect of DDoS, higher the chances of server resources exhaustion and being unavailable. Usually DDoS is launched by the distributed attackers to minimize their identity or to remain unrecognized while attempting to overload the target to make it unresponsive.DDoS also differs from DoS in the kind of attack launch. There are several DoS attack tools like Low Orbit Ion Canon and other network scripts to start the attack execution. DDoS are launched either by distributed attackers or by distributed or compromised hosts acts as botnets. These botnets are the compromised cluster where in each physical machine will be injected a malware, so that the legitimate user of the machine would not be recognized that they involved in the attack. Here the attack requests are continuously bombarded towards the servers. The machine involved in the attack can be either computers or smartphones or network routers.

2.1. Types of DDoS Attack:

DDoS attack types are generally divided into three general categories: They are Volume based attack, Protocol based attack, Application layer based attack. *Volumetric Attacks* are the kind of attack where the attackers attempt to launch immense spurious requests to acquire the bandwidth with the notion of making the server unavailable for the intended users. For doing so, attackers simply congest the network by breaking the link between cloud resources and other users network or form internet to make the server offline.

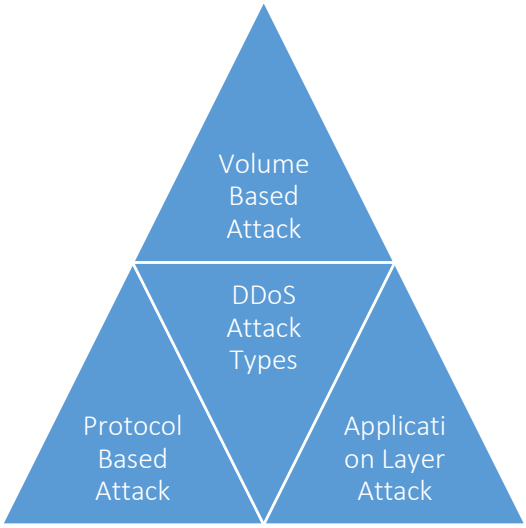


Figure 2. DDoS Attack Types

Protocol Attacks are another different kind of attack who attempt to destruct the infrastructure services like load-balancer's configuration and other firewall connection state logs. This protocol based attacks aims to bring down even millions of connections by leading to TCP state exhaustion. *Application Layer Attacks*are the most dangerous and highest threat of all other types. This kind of attack is hard to detect as the attack rate will always be as low as possible which is difficult to detect and prevent. HTTP GET Flood is the most common flooding attack and there are several tools like slowloris and Rudy. There are other kinds of attacks like DNS query flood, slow attacks which attempts to damage server by overloading the resource-intensive request processing.

These kinds of attacks when launched towards any server will lead over usage costs for subscribers and operational damages, data loss for service providers. The rate at which these attacks launched would exceed 200 Gbps. But with the current server's infrastructure 20 to 40 Gbps are enough to bring down the server completely.

2.2. Variants of DDoS Attack:

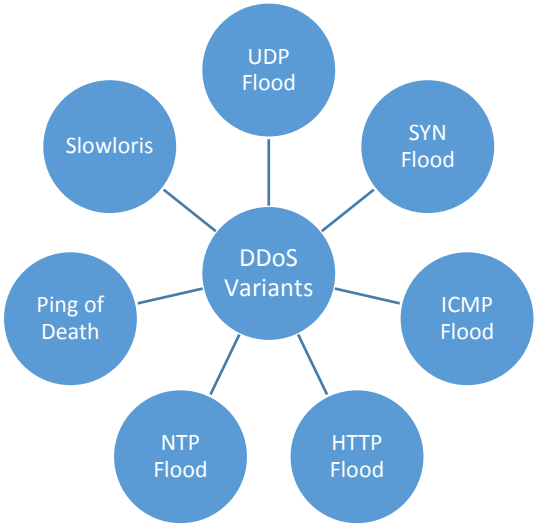


Figure 3. Variants of DDoS

DDoS attacks launched with several variants with the only aim to undermine the server's resources completely. Some variants of DDoS attacks are ***UDP Flood*** is the type of attack floods which leverages User Datagram Protocol (UDP) by launching UDP packets to the random ports of remote host. This causes the remote host to listen and check for the application but finds the ICMP Unreachable Destination and turn to non-accessible application. ***ICMP (Ping)*** *Flood* is another kind of DDoS variant which shoots ICMP echo request packets continuously with very less inter-arrival rate *i.e.*, before getting response from the server. This creates queue at server and also bandwidth congestion so, server would not be able to handle the requests and leads to server shutdown. ***SYN Flood*** is another kind of flooding which makes use of TCP connection sequence as adverse effect, here the attacker launches the SYN request which then responded with SYN_ACK, but the attacker without responding to the ACK, keeps overloading with SYN requests, this cause the queueing and resource or session leakage and overflow and in turn eventually cause denial of service. ***Ping of Death*** is launching the malicious ping towards victim. This kind of attack malforms the packets which is of irrelevant headers or size (bytes). At data link layer, the splitted packets are reformed or reassembled but end up in recognizing the irrelevant packet. This consumes much memory buffer and avoids the inflow of legitimate users. ***Slowloris*** is again a silent attack which targets in holding as many connections as possible at victim server and make it open for prolonged period of time. By still kept opening of connections at target server makes the concurrent connection pool overflow, which blocks legitimates to access the server resources. ***HTTP Flood*** is one of the common attack launched towards any webserver. Here, the webserver is forced to allocate the resources for malicious request too, when this allocation continues, the percentage of legitimates served drastically reduced. Aboosaleh Mohammad Sharifi *et. al.*, (2012) also discussed about the availability issues of DDoS in cloud computing.

3. Illustrative Cases of DDoS Effect in Cloud Computing

DDoS would lead to business discontinuance as it remains serious threat at various user group and cloud service. DDoS is not only remains as a threat to retailers, manufacturing and logistics, health care data support, financial services and big data process gaming

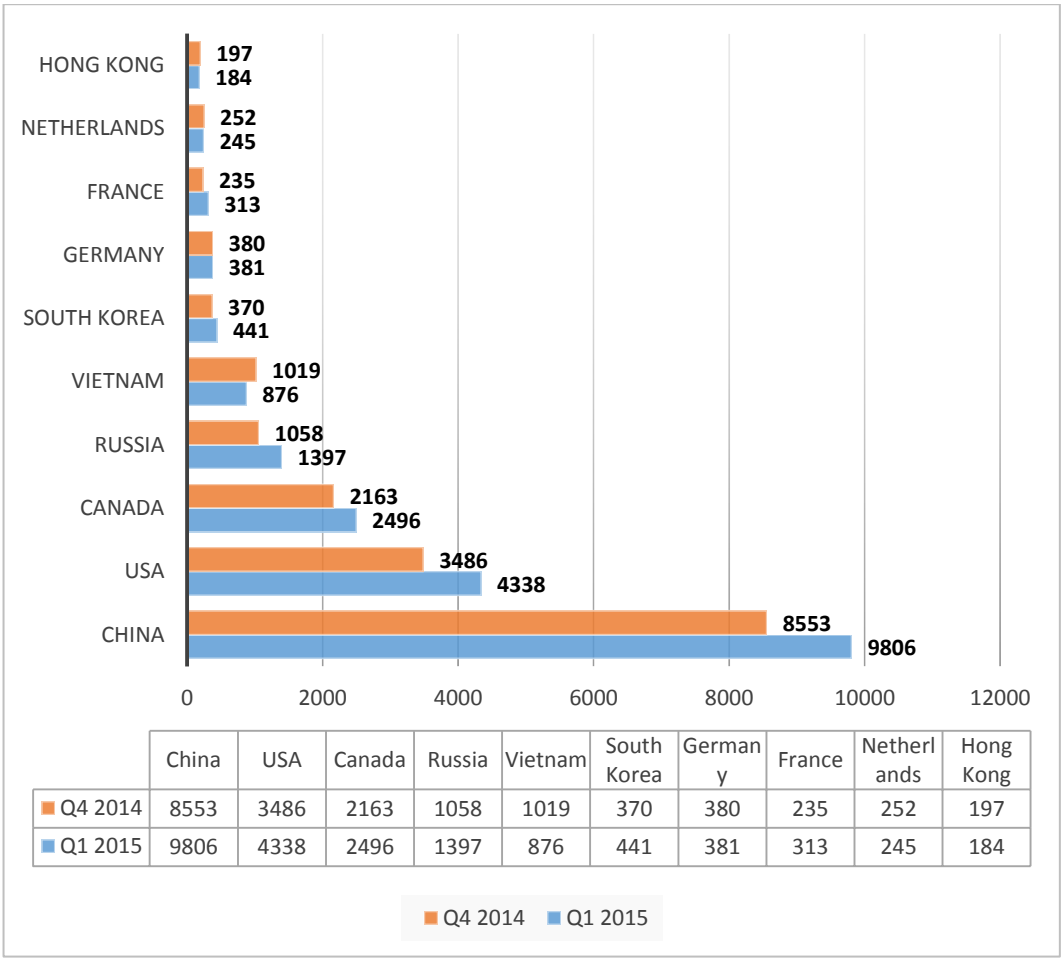
companies to subvert the servers' performance but it also outwits the legitimate users from using the regular and basic need for availability and make them remain inaccessible for the subscribed services. Losing the sensitive information by the DDoS attack launchtowards mission critical business applications will lead to permanent resource outage or to remain service offline from the day-to-day service needs such as email, salesforce automation, CRM and many others. An Example of DDoS attack towards cloudflare is 65Gbps DDoS which is a big attack, easily in the top 5% of the biggest attacks. When an attack is 65Gbps that means every second 65 Gigabits of data is sent to cloudflare network. That's the equivalent data volume of watching 3,400 HD TV channels all at the same time. It's a ton of data. Most network connections are measured in 100Mbps, 1Gbps or 10Gbps so attacks like this would quickly saturate even a large Internet connection. Another Example of DDoS towards Microsoft Datacenters which is a DDoS attack made headlines in March of 2013, when attackers used DNS amplification to attack the Spamhaus spam prevention service with as much as 300 gigabits per second (Gbps) of traffic.

3.1. After-effect of DDoS

When any application existing in public domain turn unavailable, it would be a business loss, loss of fame and revenue loss for product owners. When the same business critical application turns unavailable, all the operations related to the business will quit and cause a serious chain reaction of loss to all the subsidiaries. Unless and until the strong defense network in place, these kind of attacks cannot be tolerated by the existing architectures and to serve resilient to the subscribers on-demand basis.

4. Motivation of the Study

The work described in this section is related to areas including Distributed Denial of service, Cloud computing and its security challenges which includes the discussions related to botnets, spoof, aggressors related availability issues with respect to agents. The significance of Cloud computing motivates us to pursue the research towards cloud computing. The security issues faced by cloud computing poses the service and resource unavailability at the intended time. DDoS is the top most attack criteria for making resource unavailable. In order to minimize and prevent DDoS against DC and to make DC to serve resilient, several causes and cases of DDoS must be detected at the earliest and outwitted temporarily. This resource protection helps cloud service provider to maintain privacy and being highly fault tolerant. The considered cases are namely DDoS and similar kinds of overload threats like botnets, aggressive legitimates and spoofers. The necessity of research can be understood by looking at the below statistical update of DDoS by securelist.com website. The data is recorded at Q4 2014 and Q1 2015. With this kind of DDoS data statistics, the importance of DDoS prevention mechanisms can be understood as an essential activity for any cloud service provider. Figure 4 shows the DDoS Attempts from the top 10 countries list. Even Microsoft blog insists that 30 Mbps attack when left undetected it could lead to service availability. Recognizing the user's identity towards any network is most important to provide service to them. Kerberos is one of the known network authentication protocol for validating the user. Eman El-Emam *et. al.,* (2009) enrich the mechanism of existing Kerberos system. Kerberos uses Ticket generation server for ticket exchange between any communicators. On successful ticket generation, the service grant request is shared between client and server. The enhancement to the existing scheme and version is the update of hashing algorithm and encryption algorithm for the secret key block generation. YudhaPurwanto *et. al.,* (2014) proposed anomaly detection scheme which takes different overload into account, process the traffic requests, pre-processing them, and detect the anomaly traffic.



	China	USA	Canada	Russia	Vietnam	South Korea	Germany	France	Netherlands	Hong Kong
Q4 2014	8553	3486	2163	1058	1019	370	380	235	252	197
Q1 2015	9806	4338	2496	1397	876	441	381	313	245	184

Figure 4. DDoS Attempts - Statistical Data (as per securelist.com)

Trust, Belief, confidence plays vital role in relying anyone's character. Prolonged genuine behaviour improves trust and dishonoured behaviour degrades the trust value. With this notion, the trust computation is made as an authentic factor for learning the incoming requestors' behaviour. Eschenauer *et. al.*, (2004) proposed a framework for, the evidence based trust management. This considers the trust as a set of relationship between any two parties with the support of evidence. One way to generate evidence is through public-key cryptography. One of the entities in the network can create evidence for itself and for others. In order to create the evidence, the creator entity creates a piece of entity and signs it with the private key. It mentions its validity period and shares it to others with a public key for identification. Here the drawback is an entity could also revoke the shared evidence. Since the revoking option could allow any anonymous to create evidence and to revoke it, this would create chaos in the network.

DDoS attacks are most critical category of unavailable attacks, as they are easy to launch and hard to detect. There are several DDoS tools available like Trinoo, Wintrinoo, LOIC, HOIC, R-U-Dead-Yet (RUDY), XOIC, HULK (HTTP Unbearable Load King) and Tor's Hammer. Attackers bombard a large volume of packets to saturate the server's network resources and eventually bring down the cloud service to a halt. UDP flood, ICMP flood, DNS flood are the widely used DDoS flood in layer-3 attack T.peng *et. al.*, (2007). UDP flood attack leverages UDP packets to congest random or specific ports of the server keeping the server application busy in listening at the ports and when it does not find any application waiting for that ports it ultimately sends a "destination unreachable" ICMP message to spoofed source addresses. In ICMP flood attack, a large

burst of ICMP echo packet ('Ping' flood) is sent to destination that congest the bandwidth of server's bandwidth as victim needs to reply all echo requests. Based upon the severity of the attack, the server side services can be slow or completely crashed down. UDP and ICMP floods are detectable and can be prevented by setting threshold values at border routers where routers only allow UDP/ICMP packets up to threshold rate.

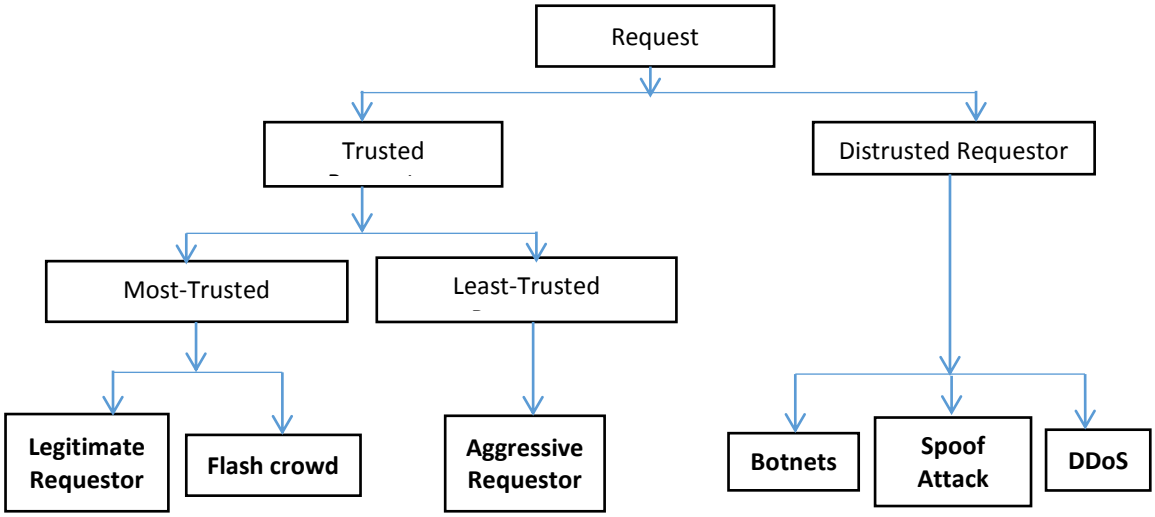


Figure 5. Varieties of Requestor (As Per Trilateral Trust Based Defense Mechanism - NChSN Iyengar *et al*.,)

Cloud computing always suffice dynamic resource allocation and release which requires the large scale computation. Node selection for any submitted task requires the optimal resource allocation based on the properties of the submitted task. BrototiMondal *et. al.*, (2012) insists stochastic Hill climbing can be used for incoming job allocation to servers or virtual machines. A stochastic and local optimization is a simple loop for finding the best fit node among neighbours. This loop breaks until there is no neighbour to be found which is most suited to the current submitted task requirement. This search keeps going uphill for best fit until it finds the largest resource pool available. SO, initially, the search is made uphill and then the slight change is made to the available configurations once all the resources are indexed, which is a beneficiary act of scoring the resources after the evaluation. The index table is created for the VM, status of each VM is marked either as Busy or available, whenever any task arrives, best fi VM is parsed among all available resources and allocated. Deallocation is again indexed for further and improved resource utilization. Zhen Xiao *et. al.,* (2013) identified skewness which is a metric to measure the server's unevenness related to resource allocation. Resource utilization can be improved by reducing skewness by the combinatorial effect of different types of workload. The load prediction algorithm which constantly varies whenever there is change in resource allocation, which can probabilistically measure the resource requirement based on the kind of task submission.

In order to protect the DC resources, at any point of time, the overload should be avoided. Pattern matching of incoming load reveals the VM arrangement for precise resource management and requirement prediction. KashifuddinQazi *et. al.,* (2014) identifies the framework which predicts the heuristic cluster behavior and redistributes the VM and physical machines. The freed up physical machines are re-organized and re-distributed. Chaotic time series is used for optimizing the resource allocation and monitoring the incoming load. Chonka *et. al.*, (2009) recognized the stability states, where the non-linear function maps the state of incoming traffic. Against the incoming traffic,

the combined traffic is analyzed and the chaotic deviation is captured and also the change in normal and abnormal incoming traffic is then processed to segregate the traffic requests. Dimple et al (2009) proposed a framework which contains Mobile Agent, Host Agents, controllers and Filters to detect and protect the resources from DDoS attackers.

5. Comparative study of DDoS Defense Mechanism

This Section consists of comparison and analysis of various DDoS mitigation schemes which directly or indirectly relates cloud computing environment.

5.1. Comparative Study of Existing Related Works

Table 1. DDoS Defense Mechanisms Comparative Study

Related Work	Proposed Feature	Limitations
S. Ahmed and S. M. Nirkhi (2013) proposed Fuzzy logic based forensic analysis	Forensic analysis based upon data stored in log files, configuration settings, routing tables *etc.*	Limited to small level attack
D. Vydekiand, R. and S. Bhuvaneswaran (2013) proposed Fuzzy inference system based anomaly detection	Specification and anomaly based detection from Data packets and Control packet based features	Restricted to blackhole attack only
V. Manoj *et. al.*, (2012) proposed Trust and fuzzy logic based detection system	Uses network level data for cryptographic algorithm and trust based anomaly detection.	Only malicious node detection in collaborative way
N. Jeyanthi *et. al.*, (2012) proposed Packet Resonance Strategy (PRS) to detect and prevent DDoS attack from Spoofed addresses	PRS implements a defense mechanism consisting of two levels: packet bouncer and packet transit. It permits access to cloud datacenters only if remote clients satisfy initial authentication at both the levels. This light weight solution is able to detect malicious packets from spoofed addresses and discards those packets at DC's firewall.	It obtains intended communication channel for authenticated users. Also tracing the attack source to block further traffic flow from those addresses was not discussed
R. Vijayan *et. al.*, (2011) proposed Energy based trust solution using fuzzy logic for anomaly detection	Uses network packet data as source for anomaly detection	Not collaborative and response system is not given
Chen Qi *et. al.*, (2011) proposed a confidence based filtering (CBF) method for mitigating	CBF is a packet filtering method that generates a nominal profile for normal, legitimate packets during non-attack period and	This method scores the packets based on some characteristics concurrently appeared in

DDoS attack	evaluates the score of packets during attack period to decide if the packet can be discarded or not. This allows dynamic packet filtering with high accuracy in very less time.	legitimate packets. But specific number of single attributes are not defined that need to be selected. To accumulate the confidence values of attribute-value pairs, a database is maintained at server side to store them in a 3-dimensional array due to which computing speed can be affected.
Chi-Chun Lo *et. al.,* (2010) proposed a cooperative intrusion detection system (IDS) framework.	Cooperative agents from IDS deployed in each cloud environment exchange alerts if one IDS identifies any attack. Alerts coming from different regions are collected by alert clustering module and decision about accepting the alert is taken based upon severity of the attack. This system protects cloud environment from single point of failure.	Implementation of the cooperative agent and the majority voting system include much computational effort to existing defense system. Eventually, the system can experience high computation time and low detection rate of attacks. Also, to build this model, special cloud infrastructure is needed.
AmanBakshi *et. al.,* (2010) proposed IT virtualization strategy to secure cloud environment from DDoS attack	SNORT like IDS in virtual machines is used to analyze incoming and outgoing packets and to evaluate with known signature. If DDoS attack is detected, target application is shifted to other virtual machine at different data center and packets from malicious IP addresses are blocked. This approach prevents DDoS attack in virtualized cloud environment by securing applications running in virtual machines.	SNORT kind of IDS identifies known attacks; hence all kind of DDoS attacks are not detected and prevented in virtualized environment.
Kleber Vieira *et. al.,* (2010) proposed a neural network based anomaly detection scheme in grid and cloud computing	An Artificial Neural Network based anomaly detection mechanism having an audit system to secure the cloud from attacks.	It cannot work efficiently if training data is limited. Also intrusion detection takes much time.

A. Visconti and H. Tahayori (2010) proposed Type-2 fuzzy set based algorithm for detecting misbehaving nodes	Collects sample data of various network parameters in distributed environment for partial-anomaly based detection from misbehaving nodes.	Routing protocol is not specified, simulation result is not given
Damian Watkins (2004) proposed Fuzzy Sets based Agent communication	Collect packet data from data stream for misused based detection; independent and collaborative	Routing protocol is not specified, prevention scheme could be presented
SampadaChavan *et. al.,* (2004) proposed a neuro-fuzzy based intrusion detection system	An Artificial Neural Networks and Fuzzy Inference System based defense mechanism that uses SNORT for real time traffic analysis. Signature pattern database is built from supervised and unsupervised learning method.	Significant training time can restrict it to be used in a dynamic network.

5.2. Experimental Comparison

The research related studies helped in analyzing some of the works related to our field of our work and also the comparison is much useful in identifying the way of DDoS mitigation and its limitation. This helps any researchers or the users who attempt to acquire certain mechanism adapt to their network to escape form DDoS threat. But these existing studies are not the only ways to mitigate DDoS. We have also made an in-depth study and analysis of five of the DDoS related existing research work as a reference where each of the mechanism is varied in their implementation and methodology and to spot the better one among them.

5.2.1. Methodology 1

A Multilevel Thrust Filtration Defending Mechanism monitors for any requests from any client group interests in requesting resource from DC, they send the unique client ID to Intermediate Web Server (IWS), which here acts as a lookup server. This IWS is maintained by CSP. So, there is no need of any third party support for connecting the clients and DC. This IWS holds information about several DCs. When the requester requests IWS, it finds the incoming client ID is registered or not, if registered, the encrypted form of message is sent back to the client with the particular ASN's IP address which is ciphered with clients' password. Now, ciphered message recipient can be able to decrypt the Authorized Scrutinizing Node (ASN) IP address only if recipient is the intended client. So that the client could communicate further. Other requester is considered as fake requester. On consecutive failure for certain number of times, the requester is filtered at firewall.

On successful decryption, the client forwards the message sent by IWS to ASN. Now ASN validates the digital signature of IWS by decrypting it. On successful validation, the certificate is generated which contains the session key and Timestamp. This is valid only the particular concerned client. This generated certificate is stored at ASN and also sent to the client. When client decrypt the ASN's response, client gets session key and communicates with DC via ASN. Here, ASN acts as an exclusive protection layer which the requester is unaware. So, the requests cannot bypass ASN and reach DC. This ASN

protection chain helps in deploying the detection mechanism at the cloud boundary to detect the abnormal traffic condition earlier which is much cost effective.

5.2.2. Methodology 2

Trilateral Trust Based Defense Mechanism Whenever the clients require the service, they initiate the service request to the subscribed cloud service provider's DC, which is routed to Traffic Injection Rate Detector (TIRD). At TIRD, the maximum number of requests ($TIRD_{max}$) that the DC can handle is preset based on the cloud service provider configuration.

If the number of request exceeds the $TIRD_{max}$, the traffic condition is considered 'abnormal'. TIRD redirects the client request to the firewall. Firewall verifies the log that the incoming client is defaulter for service provision. If the incoming client is not a defaulter, then the client ID is forwarded to Mutual Trust Initiator (MTI) which is a database server that holds the clients secret key. For MTI Session ID is generated and encrypted with the secret key and sent back to the requestor. Now at requestor end, the session ID can be obtained only if the requestor is valid and legitimate requestor as the secret key is shared only between MTI and requestor. When the client sends back the session ID to MTI, the session is established. Otherwise, the behaviour is considered as resource hunger activity and the credit point is considerably reduced.

Once the session is established, the clientencrypted Trust Tag is passed to the Trust Tag Validator (TTV) where the encrypted trust tag is decrypted with a secret key and the behaviour history can be monitored. If the incoming client is a defaulter, then particular client will not be served until the session expires. This scheme assures that the same client who is defaulted is not given a chance of being served continuously. This allows new users to be served. The trust tag reviews the behaviour history and reports the character of the requestor. At Credit Points Updating Module (CrPU), based on the behaviour reported by TTV, the CrPU classifies the requestor as legitimate behaviour and resource hunger behaviour. The resource hungers' credit points are reduced considerably. If the behaviour is legitimate and calm, the credit points are increased. Once the requestor passes the validations at these three different views, then the requestor is considered legitimate.

Now the incoming traffic from CrPU to load balancer is considered legitimate. At Load Balancer (LB), all the incoming requests are queued and forwarded to the DC based on the DC load, so that the DC is available to all legitimate requestor at all time. It is necessary requirement that all the new requestor towards DC must be generated secret key and shared between DC and requestor via same cloud service provider channel. Subsequent communication will be authenticated based on session ID which monitors only active sessions, thus reduces traffic monitoring overhead. It would be common that digital certificate would be lost at the traffic prone networks, so the number of attempts and the timeout period to accept the certificate as a valid depends on cloud service provider network conditions which can also be configured. Higher the traffic congestion is proportional to increasing the attempt of accepting the certificate as a valid. Here MTI acts as a key manager and which is also a scalable database server, which also suffice shared secret key validator for any service requestor from the requestor and assuring the integrity by validating a digitally signed certificate.

The Trilateral Trust mechanism involves three sequential traffic threat notification levels for authenticating the incoming requestor as a trusted client or threat. At each level, some kind of threat is detected and the threat traffic reduced and narrowed to successive levels. Upon detecting the high rate of attack-prone sources at earliest reduces the traffic congestion at DC. This ultimately improves the DC resources available only for legitimates without contaminating other expensive resources for attack-prone traffic threats.

5.2.3. Methodology 3

A Fuzzy Logic Based Defense Mechanism is the design of a hybrid fuzzy defense mechanism against DDoS attack is based on the statistical behaviour of parameters of network protocols. The plan is to consider parameters from network level as well as application level protocols that would help to depict the traffic pattern in a DC server. DDoS is not a single kind of network attack but a general name of different kinds of attack strategies that exploit the loopholes in existing security systems and protocols to disrupt the victim's resources. We would select the vital network parameters that change significantly during an attack phase and hence its pattern gives an essential clue to detect denial of service attack from normal traffic. Before launching the attack, an attacker sends ICMP Echo packets to find the machines which are vulnerable to security threat and gains their access. Once those machines are compromised, those become the agents to consolidate a DDoS attack towards a single destination. During the attack period the destination IP address becomes common in each packet trace. The self-similarity of each network that exists regardless of network type, protocols, topology and packet size plays a crucial role in statistical anomaly detection.

The working phases of the system can be divided into four: **Learning Phase:** In this phase the inference rules are designed and fed to fuzzy systems. First the required parameters or inputs to the system are declared. These parameters are the packet characteristics that change considerably during the DDoS attack. Fuzzy system learns to make decision based upon data fed and determines the traffic class. **Traffic Analysis:** In this phase, the fuzzy based defense system monitors the traffic dynamically, analyzes and evaluates the traffic class based upon inference rules. The fuzzy rules are defined in conditional way in IF-ELSE form to determine the logic. Here the rules for defending DDoS attack are flexible and can be modified based upon type of attack and the network parameters change due to the attack. **Anomaly Detection:** Fuzzy system determines the traffic class and generates alarms if anomaly is found. **Attack Prevention:** Border routers are asked to discard the packets from malicious sources. Distinguishing a DDoS attack from flash crowd and shrew attacks is a difficult job that any DDoS defense system should take care of. These are legitimate traffic patterns that create sudden surge in network packet flow when a large number of valid users try to access the service concurrently. These events do not reach any harm to data centers and does not stay for long period of time.

5.2.4. Methodology 4

An Effective Layered Load Balancing Mechanism considers several requestor group who can be of one of the several groups requesting several types of requests. Once requestor initiates request Traffic Range Perceiver (TRP) helps in sensing the incoming request traffic rate. This TRP acts as the early alarm system which identifies and classifies the traffic rate as normal and abnormal. The traffic rate is identified and then fed into firewall which at the initial stage directly allows the requests to bypass as the firewall has not informed about the incoming requests. Once the incoming request bypass firewall and reaches Authenticity Predictor (AuthPr), the incoming client requests types are identified and processed accordingly. The incoming request types are recognition requests, acknowledge requests, service requests. All the incoming request types are configured at web services for dynamic identification at AuthPr. If the incoming requests are new requestor they are queued separately at Restrain Timer which is to authenticate the incoming requestor activity. Restrain Timer (ResT) is contains two distinguishable queues to increase the service rate for legitimate clients. One of the queues holds the new requestor requests, and another queue is for registered requestor requests which not only optimizes the service rate and also allows new requestors at appropriate time. The authenticated requestors bypass the Restrain Request Manger (RRM) module and reaches

Load Balancer (LB), Here the LB is again broken up into two modules: they are overload Diminishment (oDim) and Instantaneous Load Balancer (ILB). The reason of LB being splitted into oDim and ILB is because of the new registration requestor joins the traffic at Authenticity Predictor, which does not give any information about the character of incoming requestor. So the oDim, helps in detecting the overload if incase the new requestor attempts to overload the DC. Other kind of overload condition is detected at ILB. ILB is a very fast and efficient module to handle with almost any kind of request as it already gets some kind of information from the previous modules as buffer information and reports firewall to filter the requestor for certain period of time.

5.2.5. Methodology 5

Chaotic Theory based Defensive Mechanism is a proposed detection mechanism that has three modules namely Network Traffic Analysis, Anomaly Detection and overload classification to validate the requestors' characteristics. The requestors' request traffic always bypasses Network Traffic Analysis phase where the state of stability is determined. The traffic stability state is derived based on the heuristics. The analyzed traffic is allowed to anomaly detection module which considers Lyapunov's stability theorem for the proposed dynamic traffic system, implies to concern the point at which the state of stability of solution which is near to equilibrium. Based on the stability state and the probability measure of the uncertain traffic condition, the overload condition is predicted as normal or abnormal. Then the cause of overload is precisely predicted and the attack cases are filtered, non-attack cases are allowed to access DC resources.

5.2.6. Overall Methodologies Comparison

This comparison aimed at detecting and preventing Distributed Denial of Service attack, and also the overload behavior to diminish the major attack. Otherwise, leads to DC performance degradation and also DC service shutdown. This

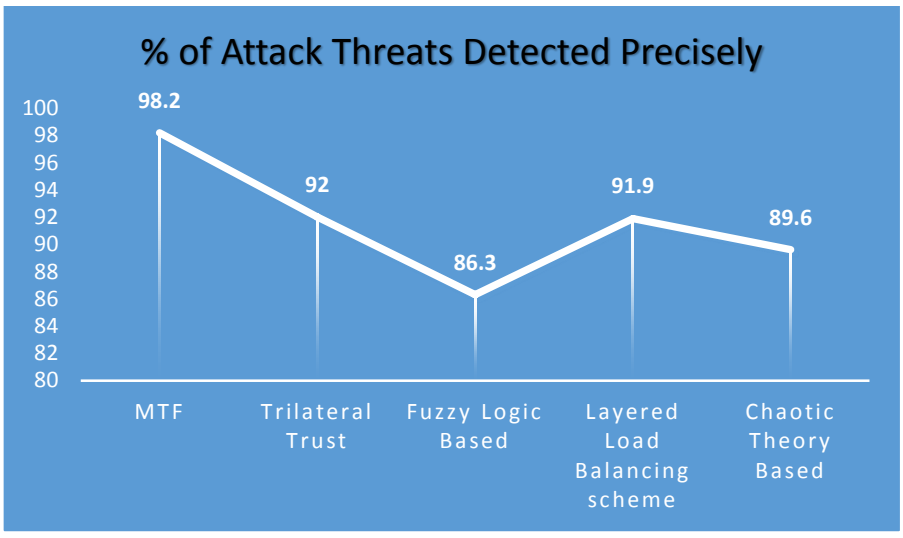


Figure 6. A Research Summary (% of Attack Threats Detected)

causes the services unavailable to the legitimate users on demand and the cloud environment will lose its fame. The attack can be invoked through several modes. Even a legitimate user can be compromised by spoofing the IP address and cause burst in traffic. These different modes of attack initiation have been taken into consideration which is detected and prevented by the novel mechanisms proposed in this work.

For the better way of summarization, the important result and sole aim of this research study is displayed at figure 6. Incoming requestors can be malicious or non-malicious, but the malicious overload attacker is not only reason of DDoS traffic overload, non-malicious case of overload could also be the reason of DC service availability. By having this notion, traffic is consistently monitored and analyzed based on the incoming traffic so as to segregate the incoming traffic and different treatment is provided for different kind of incoming requestor group. This positively improves performance which in turn improves profit and protects the valuable DC resources.

Table 2. Summarization of the DDoS Mitigation Mechanisms

Multilevel Thrust Filtration: A DDoS Defense Mechanism	Application of authentication protocol to cipher the requestor transaction to uniquely identify the requester and allows in. Moreover, it also detects and filters four different kinds of overload conditions such as: botnet, DDoS, Flash crowd and Spoof attack, detected at various levels. Considering several overload condition implies improved traffic analysis and restricting the overload traffic. Improved profit and Quality of Service.
Trilateral Trust: A DDoS Defense Mechanism	A Delegated way of handling incoming traffic by making use of Trust Tag for each registered requestors. Trust Tag holds heuristic information for determining the behaviour of any requestor. Monitoring the legitimate requestor is an added advantage with the notion whether the legitimate could turn out to be an overload requester. Improved profit and response time, reduced network overhead by minimizing the network information fetches of any requestor.
Fuzzy Logic Based DDoS Defense Mechanism	Predefined traffic parameters that vary significantly between a normal and attack traffic pattern and fuzzy rules are defined based on incoming traffic. Improved Accuracy, sensitivity, and reduced false case rates. Better traffic filtration results in improved response time. Distinguishes flash crowd and DDoS attack traffic and acts accordingly.
Layered Load Balancing Based DDoS Defense Mechanism	Effective load factor computation by segregating the requestors based on the registrant priority. DC Information caching improves response time and reduces the latency of analyzing the load information on demand. Intra DC (VM Load) and Inter DC Load balancing is faster with the help of updated Informative Resource Repository. Reduced network overhead, consistent filtration at each layers improves detection efficacy.

Chaotic Theory Based DDoS Defense Mechanism	Classifies attack, non-attack cases based on network traffic analysis via chaotic deviation. Precise traffic state prediction by Lyapunov's chaotic equation. Improved Goodput and reduced request traffic queuing at DC. Reduced False Positive and False Negative rates of requestor traffic.

6. Conclusion

These researches aimed at detecting and preventing Distributed Denial of Service attack, and also the overload behaviour to diminish the major attack. Otherwise, leads to DC performance degradation and also DC service shutdown. This causes the services unavailable to the legitimate users on demand and the cloud environment will lose its fame. The attack can be invoked through several modes. Even a legitimate user can be compromised by spoofing the IP address and cause burst in traffic. These different modes of attack initiation have been taken into consideration which is detected and prevented by the novel mechanisms proposed in this work.

Here the overall research result can be found in terms of percentage of attack threats detected at the time of our simulation. The results are provided as the average of three runs for each experiment and the data is computed based on the actual threats detected from the overall threats involved in DDoS.

Incoming requestors can be malicious or non-malicious, but the malicious overload attacker is not only reason of DDoS traffic overload, non-malicious case of overload could also be the reason of DC service availability. By having this notion, we consistently monitor and analyse the incoming traffic so as to segregate the incoming traffic and different treatment is provided for different kind of incoming requestor group. This positively improves performance which in turn improves profit and protects the valuable DC resources.

References

[1] A. M. Sharifi , S. K. Amirgholipour, M. Alirezanejad, B. S. Aski and M. Ghiami, "Availability challenge of cloud system under DDOS attack", vol. 5, no. 6, **(2012)**, pp. 2933-2937.
[2] E. El-Emam, M. Koutb, H. Kelash and O. F. Allah, "A Network Authentication Protocol Based on Kerberos", IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 8, **(2009)**, pp. 17-26.
[3] Y. Purwanto, Kuspriyanto, Hendrawan and B. Rahardjo, "Traffic anomaly detection in DDos flooding attack", 8th International Conference on Telecommunication Systems Services and Applications (TSSA), Kuta, **(2014)**, pp. 1-6.
[4] L. Eschenauer and V. D. Gligor, "J. Bara. On Trust Establishment in Mobile Ad Hoc Networks. – Security Protocols Springer", **(2004)**, pp. 47- 66.
[5] T. Peng, C. Leckie and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems", ACM Computing Survey, vol. 39, no. 1, **(2007)**, pp. 1- 42.
[6] B. Mondal, K. Dasgupta and P. Dutta, "Load Balancing in Cloud Computing using Stochastic Hill Climbing-A Soft Computing Approach", Procedia Technology, vol. 4, **(2012)**, pp.783–789.
[7] Z. Xiao, W. Song and Q. Chen, "Dynamic Resource Allocation Using Virtual Machines for Cloud Computing Environment", IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 2, **(2013)**, pp. 1107-1117.
[8] K. Qazi, Yang Li and A. Sohn, "Workload Prediction of Virtual Machines for Harnessing Data Center Resources", IEEE 7th International Conference on Cloud Computing (CLOUD), Anchorage, **(2014)**, pp. 522 – 529.
[9] A. Chonka, J. Singh and W. Zhou, "Anomaly Detection of Distributed Denial of Service Attacks by Non-Liner Dynamics", IEEE Communications letters, vol. 13, no. 9, **(2009)**, pp. 717-719.
[10] S. Ahmed and S. M. Nirkhi, "A Fuzzy approach for forensic analysis of DDoS attack in manet", International Journal of Advanced Computer Science and Applications, vol. 4, no. 6, **(2013)**, pp. 193-198.

[11] D. Vydeki and R. S. Bhuvaneswaran, "Effect of clustering in designing a fuzzy based hybrid intrusion detection system for mobile ad hoc networks", Journal of Computer Science, vol. 9, no. 4, **(2013)**, pp. 521-525.
[12] V. Manoj, M. Aaqib, N. Raghavendiran and R. Vijayan, "A Novel Security Framework Using Trust and Fuzzy Logic in MANET", International Journal of Distributed and Parallel Systems (IJDPS), vol. 3, no. 1, **(2012)**, pp. 285-299.
[13] 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 & Information Security, vol. 4, no. 3, **(2012)**, pp. 163-173.
[14] R. Vijayan, V. Mareeswari and K. Ramakrishna, "Energy based Trust solution for Detecting Selfish Nodes in MANET using Fuzzy logic", International Journal of Research & Reviews in Computer Science, vol. 2, no. 3, **(2011)**, pp. 647-652.
[15] Q. Chen, W. Lin, W. Dou and S. Yu, "CBF: A packet filtering method for DDoS attack defense in cloud environment", IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing, Sydney, **(2011)**, pp. 427-434.
[16] C.-C. Lo, C.-C. Huang and J. Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", 39th International Conference on Parallel Processing, ICPP Workshops, 2010, California, **(2010)**, pp. 280-284.
[17] A. Bakshi and B. Yogesh, "Securing cloud from ddos attacks using intrusion detection system in virtual machine", IEEE Second International Conference on Communication Software and Networks, Singapore, **(2010)**, pp. 260-264.
[18] K. Vieira, A. Schulter, C. Westphall and C. Westphall, "Intrusion detection for grid and cloud computing", IT Professional, vol. 12, no. 4, **(2010)**, pp. 38-43.
[19] H. T. Visconti, "A Biologically – Inspired type-2 fuzzy set based algorithm for detecting misbehaving nodes in ad hoc networks", International Journal for Infonomics, vol. 3, no. 2, **(2010)**, pp. 270-277.
[20] S. Chavan, K. Shah, N. Dave, S. Mukherjee, A. Abraham and S. Sanyal, "Adaptive neuro-fuzzy intrusion detection systems", International Conference on Information Technology: Coding and Computing, Las Vegas, vol. 1, **(2004)**, pp. 70-74.
[21] N. Ch. S. N. Iyengar and Gopinath G., "Trilateral Trust Based Defense Mechanism against DDoS Attacks in Cloud Computing Environment", Cybernetics and Information Technologies, vol. 15, no. 2, **(2015)** July, pp. 236-248.
[22] N. Ch. S. N. Iyengar, A. Banerjee and G. Ganapathy, "A Fuzzy Logic Based Defense Mechanism against Distributed Denial of Services Attack in Cloud Environment", IJCNIS, vol. 6, no. 3, **(2014)**, pp. 236-248.
[23] N. Ch. S. N. Iyengar, G. Ganapathy, P. C. Mogan Kumar and A. Abraham, "A multilevel thrust filtration defending mechanism against DDoS attacks in cloud computing environment", IJGUC, vol. 5, no. 4, **(2014)**, pp. 236-248.
[24] N. Ch. S. N. Iyengar and G. Ganapathy, "An Effective Layered Load Balance Defense Mechanism against DDoS Attacks in Cloud Computing Environment", International Journal of Security and Its Applications, vol. 9, no. 7, **(2015)**, pp. 17-36.
[25] N. Ch. S. N. Iyengar and G. Ganapathy, "Chaotic Theory Based Defensive Mechanism against DDoS attacks in cloud computing environment", International Journal of Security and its Applications, vol. 9, no. 9, **(2015)**, pp. 197-212.
[26] (opengroup.com) http://www.opengroup.org/cloud/cloud/cloud_for_business/what.htm
[27] D. Juneja, R. Chawla and A. Singh, "An Agent-Based Framework to Counterattack DDoS Attacks", International Journal of Wireless Networks and Communications, vol. 1, no. 2, **(2009)**, pp. 193-200.

Authors

Junath Naseer Ahamed, He is currently working as lecturer at Information Technology Department, Ibri College of Technology, Oman. His area of intrest is Cloud computing, Agent technology and Information Technology

N. Ch. S. N. Iyengar, He is a Professor, SCS Engineering at VIT University, Vellore, TN, India. His research interests include Distributed Computing, Information Security, Intelligent Computing, and Fluid Dynamics (Porous Media). He had much teaching and research experience with a good number of publications in reputed International Journals & Conferences. He chaired many Intl. Conf. delivered Key note lectures, served as PC Member/Reviewer. He is Editorial Board member for many Int'l Journals like *Int. J. of Advances in Science and Technology*, of SERSC, *Cybernetics and Information Technologies* (CIT)-Bulgaria, Egyptian Computer Science Journal -Egypt, IJCA & IJConvC of Inderscience -China, *etc*., Also Editor in Chief for International Journal of Software Engineering and Applications(IJSEA) of AIRCC, Advances in Computer Science (ASC) of PPH and Many more.