CHAPTER 2

LITERATURE SURVEY

2.1 ABSTRACT

Cloud computing is gaining acceptance for adoption and implementation among organizations, however, this new technology area is facing security, performance and availability challenges. Within Cloud, Security issues are being paramount for corporate enterprises and service providers, the DDoS attacks have the highest priority among all threats to Cloud environments. This chapter presents a review of academic literature research work on the DDoS attacks on Cloud and parameters for determining effective countermeasure strategies. This chapter also introduces a new DDoS Classification taxonomy.

2.2 INTRODUCTION

This section reviews the research publications from IEEE, ACM, Science Direct and other digital libraries between the January 2010 and December 2016 in Cloud Computing and DDoS attack areas. Research publications are surveyed based on the below keywords as:

Cloud Security   DDoS Mitigation   Detecting DDoS

Hybrid Cloud   Network Architecture   Packet Flooding

SYN Flood   TCP Flood   UDP Flood

While research work and literature surveys have already been submitted in the area of DDoS domain, this literature survey is different in the following ways.

- Wong, et al. (2014) performed the research which focused on DDoS attacks on Cloud Applications and Infrastructure, while DDoS mitigation is the main focus for this Thesis.

- Several other surveys and research papers have limited scope for example Darwish, et al. (2013) and Prabhadevi, et al. (2014).

- Consequences of DDoS attacks against a Cloud environment are highlighted in review papers by Malik, et al. (2014) while this focuses on Hybrid Clouds

- DDoS attacks on Cloud Networks are explained by Merlo, et al. (2014), while Hybrid Cloud architecture and its design is the primary focus of this research.

The illustration in Figure 2.1 below illustrates DDoS cyber-attacks on Cloud environments. Since new and more powerful attack tools are now available for launching DDoS attacks, the attack trends and security threats offered is not static which forces Cloud service providers to maintain latest defenses for being a step ahead of the most recent attacks.

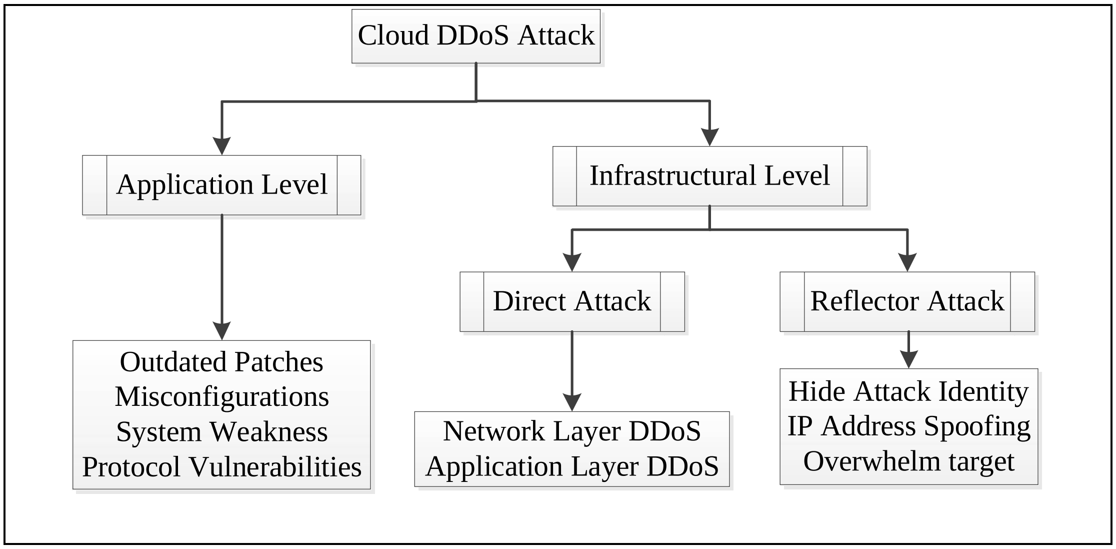

Figure 2.1: DDoS Attacks on Clouds

The table 2.1 presents the DDoS attack types, features and tools.

Attack type	**DDoS Type and Characteristics**				**Attack Tools**
	Infra	**Application**	**Direct**	**Reflector**	
ICMP Flood	√		√		LOIC
SYN Flood	√		√		TFN
UDP Flood	√	√	√	√	LOIC
HTTP Flood		√	√		DDoSIM
XML Flood		√	√		DAVOSET
Ping of Death	√		√		PING
Slowloris		√	√		Pyloris
Smurf	√			√	Nemesis

Table 2.1: DDoS Attack Types and Tools

The main focus of the cyber security attack is to be able to infiltrate, impact data center devices or alter the system and application configuration information to adversely impact the uptime, availability, reputation, productivity, quality of service and the revenue of the Cloud service provider.

2.3 REVIEW OF DDoS RESEARCH PAPERS

DDoS attack reasons range from extortion, revenge to proficiency testing and political issues or even competition among Cloud service providers. DDoS affecting pricing models is reviewed for Fraudulent Resource Consumption (FRC) exploits the pay-as-you-go pricing model by Idziorek, et al. (2012) and low rate attack evading early detection that impacts the cost pricing model by Ficco, et al. (2015). A new subtle DDoS by Merlo, et al. (2014) focuses on attacks on computing resources exhausting the Cloud center energy and ultimately increase Cloud delivery costs. HTTP and XML DDoS by Chonka et al. (2012) attacks are discussed for on SaaS web services application attacks and also examines HTTP PRAGMA and HTTP POST by Dantas, et al. (2014) attacks.

2.3.1 Network Layer Attacks

TCP Flood attacks are where Transmission Control Protocol requires a three way handshake prior to establishing actual packet exchanges with connection orientated protocol features. Whenever the connecting host sends a SYN message, it is acknowledged with a SYN + ACK and the handshaking process completes with ACK, finally establishing host to host connections. This three way handshake process is exploited by cyber-attackers by initiating half open connections, leading to huge number of transmission block allocations exhausting the kernel memory as described by Wong, et al. (2014). Network and transport layer protocol attacks to flood a host using TCP SYN, UDP and ICMP floods by Zargar, et al. (2013) is also researched exploiting TCP SYN for half open connection feature leading to large number of transmission block allocations causing exhaustion of kernel memory.

UDP Flood attacks occur at the transport layer utilizing UDP connectionless feature where packet transfer reliability is not mandatory. Protocol vulnerability impact is brought forth by Rui, et al. (2009) when initiating traffic floods to random UDP ports to online gaming portals and instant messaging applications. Wong, et al. (2014) directed huge volume of malicious traffic filling up the user response queue, displaying the connectionless and unreliability feature of UDP denying legitimate authorized users access to the hosted services. The attackers sending rate of malicious traffic cannot be regulated due to UDP's unreliability feature.

ICMP Flood attacks requires the hackers to spoof ICMP or PING originally for checking the uptime status of any device or system, maliciously redirecting huge number of ICMP packets as Ping floods and Smurf attacks to hog the bandwidth, consume resources and finally crash the targeted server system. The DDoS attacks focus on flooding a predetermined target by sending a wave of malicious and malformed data packets to overwhelm bandwidth and computing resources resulting in unavailability of the targeted Cloud system as described by Choi, et al. (2013).

2.3.2 Application Layer Attacks

Cloud Application layer is targeted by HTTP Flood attacks. This is performed by use of high rate malformed HTTP packets web packet in order to overwhelm the web application server. These consume the target Cloud web server resources, preventing legitimate authenticated users from accessing the Cloud service. Mitigating such attacks is a huge challenge as these attacks are mostly stealthy and consume very little bandwidth. The target server gets inundated with HTTP and XML floods which appear as legitimate GET and POST requests.

XML Flood Attacks are performed when Cloud users and service providers deploy use of Simple Object Access Protocol or SOAP messages to initiate the Cloud session, these SOAP messages are written in XML to work with HTTP with any platform as proposed by Karnwal, et al. (2012). XML wrapping attack by Gruschka, et al. (2009) is described by changing the XML tags on Amazon EC2 Services. This enabled unauthorized access to sending spam emails to Amazon EC2.

Reflector Attacks are carried out by spoofing an IP Address to send requests to large number of reflector hosts. These hosts in turn send the response to the target by Darwish, et al. (2013), resulting in the targeted server being flooded with amplified requests from the hosts as shown by Bhuyan, et al. (2015), SYN ACK RST and DNS floods as described by Arukonda, et al. (2015).

Karnwal, et al. (2012) proposed a filter tree methodology for mitigating HTTP and XML floods on application layers detected in user resource queries when performing SOAP messaging requests. IP trace back and use of flexible deterministic packet marking of SOAP messages is performed with block listings of IPs provided by Cloud Defender. HTTP DDoS attack is detected in first four stages and the XML DDoS Flood attack is identified in the last stage.

Lonea, at al. (2013) deployed a virtual machine based intrusion detection with graphical interface to monitor Cloud fusion alerts by using Eucalyptus Cloud architecture as front end and MySQL Database backend. Attacks are captured by Barnyard tool while using SNORT for signature based DDoS rules. Stacheldraht tool is utilized for generating the resource depletion data packets. These packets consist of UDP, TCP SYN and ICMP floods. These attack packets are captured during the attack and stored in the central MySQL database. However, a limitation in this signature based approach is that unknown or zero day attacks could not be detected.

Bakshi, et al. (2010) proposed Intrusion Detection based on Signature detection for DDoS by using virtual machines running SNORT to analyze real time traffic at both in bound and out bound ports. The framework identifies the attacker's IP Address and auto scripts an Access Control List configuration to drop the data packet of the IP Address and blacklisting it immediately. Gul, et al. (2011) have mentioned that to handle a large packet flow, an intrusion detection model that analyzes and reports on the attack packets is utilized. These reports should be shared with the Cloud actors involved. In order to improve the performance of Intrusion Detection System use of multi-threading techniques is advocated. The final evaluation concluded that the use of multi thread deployment as compared to a single threaded deployment is more efficient.

Kwon, et al. (2011) also proposed Intrusion Detection based behavioral pattern detection system based on self-similarity feature and determines that normal traffic behavioral patterns could be differentiated from malicious attack traffic. The approach is to use cosine similarity option as well as use the optimum time internal for determining self-similarity. Windows server security event logs are evaluated as a pre-processor. A system alert is generated in case the self-similarity feature is invalid. The IDS checks the source IP address and the external lying points. The alert is reported and the mitigation process is initiated. The advantage of this approach is short duration of learning process and determining self-similarity on a real time basis.

Lo, et al. (2010) proposed a framework distributed inside the Cloud environment for intrusion detection. When the attack is detected by one of the IDS nodes, alerts are exchanged with each IDS nodes all across the Cloud system environment which helps detect any attack occurring inside the Cloud system.

Gupta, et al. (2013) mentioned the use of virtual machine profile optimization for attack pattern detection. Their research advocated rule based detection to match TCP SYN flood attack packets. The advantage of this proposed pattern detection is the low false positive in detecting attack signatures and use of attack labels enabling the security teams to find out the exact kind of attack experienced by the application user or the data center. However there are few drawbacks in this approach like ensuring an up-to-date signature proved to be unviable tasks, misrepresentation of the signature patterns that resulted in high false negative rate and there is the inability to detect zero day and unknown attacks.

Shamsolmoali, at al. (2014) proposed the use of a statistical filtering system with two levels of filtering. The first level of filtering involves removing the header fields of incoming data packets, then comparing the time to live (TTL) value with a predetermined hop value count. In case count values are not same, the packet is marked as spoofed and dropped immediately. The second level of filtering involves comparing the incoming packet header with a stored normal profile header.

Zakarya (2013) proposed an entropy based intrusion detection technique to identify attack flow based on distribution ratios. This study proposed use of attack packet dropping algorithm. The entropy rate identifies the attack flow, dropping the packets if the DDoS is confirmed. Cloudsim simulation shows an accuracy of almost 90%.

Vissers, et al. (2014) utilize Gaussian Model in order to preform defenses to counter application level attacks on Cloud applications using the parametric technique. The use of malicious XML content in use requests inside SOAP resulted in the DDoS attacks. Initially the detection involves HTTP header inspection to detect any HTTP floods and SOAP action inspection. Then XML content processing action is checked for any spoofing by comparing previous data. While this works very well for existing DDoS attacks, the disadvantage is the inability to detect the new age threat vectors arising from new request schematics.

Chandola, et al. (2009) proposed behavioral approach which involved collecting normal regular traffic over a period of time and use the pattern to detect any deviation from expected behavior. The patterns are grouped into three major anomalies as Point anomaly, Collective anomaly or Contextual anomaly. Point anomalies are marked for any single data instance that is considered with respect to the full data set as proposed by Prokhorenko et al (2016) for application level attacks. Collective anomaly group considers data instances for full data set while Contextual anomaly is marked for a specific context. Marnerides et al. (2015) proposed an anomaly detection system to perform statistical classification along with decomposition of signals measured using E-EMD or Ensemble Empirical Mode Decomposition. This is implemented on bare metal hypervisor and functions by taking into account both systems and network details for each virtual machine being hosted.

A Hybrid statistical model was proposed by Girma, et al. (2015) for DDoS attack pattern classification using entropy based system and covariance matrix measuring the heightened data dependency. Ismail et al. (2013) also proposed similar mathematical model having dual phase with covariance matrix to detect cyber-attacks on Cloud Applications. This had two phases, which initially involved baselining the normal traffic pattern by mapping into a covariance matrix and then comparing the current traffic with the baseline traffic pattern.

Cloud based intrusion detection technique was proposed by Lonea, et al. (2013) with the front-end server running on virtual machines hosting the data fusion methodology. The alerts are detected for each IDS and stored on the MSSQL backend database in the Cloud fusion unit. Alert analysis is done using the quantitative solution classifier and the results suggested that without any associated complexity, the proposed Cloud IDS solution managed to reduce the false negative rate and increase the detection rate.

Bedi, et al. (2012) proposed securing Cloud infrastructure from DDoS attacks using game theory. Both the legitimate and malicious virtual machine behaviors are modeled with a game inspired firewall defense.

Huang, et al. (2013) proposed a Multi-stage detection and text-based system with a Turing test to mitigate HTTP request flooding attacks. The system works in a modular fashion, with Source checking and counting modules intercepts in coming packets, the DDoS attack detection module checks for the DDoS attack, with the Turing test challenging the packets by using text based questions and answers to determine if the packet is suspicious. The attack detection module retrieves and records the traffic behavior of each virtual cluster for any suspicious traffic behavior by the inbound data packets. Turing testing module which is text-based receives the redirected blocked packets and presents a randomly selected question to the requester. Access is granted only if the question gets answered correctly. The question pool is updated regularly and the system is Linux kernel. Performance test suggested a low reflection ratio and high efficiency.

Zhijun, et al. (2006) proposed a three layer DDoS defense mechanism based on web services. Combining web server characteristics using statistical filtering using Simplified Hop Count Filtering algorithm (SHCF) and SYN Proxy Firewall at network, transport and application layer to filter malicious traffic and secure access for legitimate traffic. Limiting traffic at application layer is also applied inside a Linux kernel. These collaborative defense mechanisms provide sustained availability of the web services and can defend DDoS attacks effectively.

Ficco (2013) proposed a Hybrid hierarchical correlated security approach probes to collect and analyze information at different Cloud levels regards to architecture. Intrusion symptoms identified the cause and the target is driven by a knowledge-based ontology in this approach.

Zeng, et al. (2009) proposed an approach to block DDoS attacks based on the TCP handshake three-way process. The proposal is based on rejecting the initial inbound handshake requests as computing resources are consumed. This ensures the new normal network requests can live easy, allowing new client requests even in DDoS attack duration, thereby raising the environment's overall security capability and the system protected against DDoS Attacks.

Veronika, et al. (2012) focused on DDoS application layer attack detection, and these attacks have more impact than the traditional network layer denial of service attacks. The focus is on the cyber-attack description and aimed at detecting Denial of Service attacks at application layer. The authors also proposed few methodologies for detecting application layer attacks. While most current effort focuses on detection of network and transport layer attacks, two detection architectures for Web Application traffic monitoring are proposed to discover any dynamic changes in the normal traffic trends.

Mehmud Abliz (2011) presented an in-depth study of the denial of service problem in the Internet, and provides a comprehensive survey of attacks and countermeasures. Various DoS attack mechanisms are investigated to derive an attack mechanisms taxonomy, summarizing the challenges in DoS defense reviews and the SWOT for various proposals and provides a taxonomy of defense mechanisms.

With the aim at revealing different security threats under the Cloud models as well as network related issues and threats for Cloud Computing environment that can help Cloud researchers, Cloud Service providers and end users as shown by Disha, et al. (2013) when performing analysis of security challenges in Cloud computing. Various challenges are analyzed ranging from browser security, SQL Injection, Flooding, XML Signature element wrapping, Incomplete Data deletion, Lock-ins, Data leakage, service hijacking and denial attacks.

Arora, et al. (2012) presented an elaborated study of IaaS layers and threats to its components to determine the vulnerabilities and countermeasures. Some of the IaaS components range from SLA implementing Web Service Level Agreement framework and enforced SOA, Utility Computing implementing Amazon DevPay, Cloud Software implementing XML signatures and encryption with SOAP extensions, Network security using network segmentation at logical level with firewalls and traffic encryption as well as having network monitoring using IDS, Virtual Machine security using IPsec, VPN and Data segregation for secure provisioning and VM migrations and implementing physical security for computer hardware in data centers.

Wentao Liu (2009) analyzed DoS attack methods and attack detection technologies for network traffic and packet level content detection. TCP flood DoS attack theory with DoS attack detection program based on Winpcap for experiment is designed and the network packet generation and capture are implemented. The process of packet communication involving send/receive and analysis of packets are illustrated and the simulated DoS attack implementation mechanism and detection method is proposed.

Cornel, et al. (2012) presented an algorithm and model based on adaptive architecture to detect and mitigate DDoS attacks on web applications. Performance model predictor decides on the impact for the number of inbound requests and an inbuilt decision engine generates firewall rules for filtering the inbound traffic as well as sending suspicious traffic for further review. This traffic drops the suspicious request or moves to the next level of presenting the end user with a CAPTCHA to verify a legitimate request. Results indicate a positive result in mitigation of the attacks. The research demonstrated an adaptive architecture, an algorithm and an implementation which detects and mitigates application level DoS attacks.

Minlan, et al. (2011) present a scalable network-application profiler (SNAP) that guides the engineers to identify and fix performance related issues. This passively ensures the TCP statistics are collected, logs from socket-call having low overhead for computation and storage across shared computing resources like servers, circuits or switches and connections to pinpoint the location of the problem like TCP or application conflicts, application-generated micro-bursts, network congestion or sending buffer mismanagement. SNAP combines socket-call logs of data-transfer behaviors with TCP for the application from the network stack that highlight the data delivery. The profiler leverages the topology, network routing, and application deployment in the data center to correlate performance issues for network connections and aims to find the congested resource or problematic software component. The SNAP deployment is done in a real time production data center running over 8,000 servers and over 700 application components that uncovered over 15 major performance issue in the web application software, the network stack on the server, and the underlying network.

Malik, et al. (2012) performed a study to define a methodology for secure protection of end user critical data for Cloud providers. Various data protection techniques are analyzed. First, Mirage Image Management system which addresses the problems of ensuring virtual machine images are safe. Second, Client based Privacy Manager to help reduce threat of data loss (DL) of personal data on the Cloud, as well as providing additional privacy related benefits. Third, the Transparent Cloud Protection System designed at clearly monitoring the reliability of Cloud components. This system protects data integrity in Cloud computing by allowing the Cloud to monitor infrastructure components.

Yu-Sung, et al. (2014) proposed deploying intrusion prevention systems at access points inside the cloud environment for an individual Cloud environment. During the DDoS attack, intrusion provision system monitor incoming packets.

Akbar, et al. (2015) proposed a novel scheme based on Hellinger distance (HD) to detect low-rate and multi-attribute DDoS attacks. Leveraging the SIP load balancer for detecting and mitigating DDoS attacks is proposed. Usually DDoS detection and mitigations schemes are implemented in SIP proxy, however leveraging the SIP load balancer to fight against DDoS by using existing load balancing features is done with the proposed scheme implemented by modifying leading open source Kamailio SIP proxy server. The scheme is evaluated by experimental test setup and found results are outperforming the existing prevention schemes in use against DDoS for system overhead, detection rate and false-positive alarms.

Selvakumar, et al. (2015) proposed application layer DDoS attack detection by logistic regression using modeling user behavior. Current solutions are able to detect only limited application layer DDoS attacks while the solutions can detect all types of application layer DDoS attacks tend to have huge complexities. To find an effective solution for the detection of application layer DDoS attack the normal user browsing behavior needs to be re-modeled so that a normal user and attacker can be differentiated. This method uses feature construction along with logistic regression for modeling the normal web user behavior in order to detect application layer DDoS attacks. The performance of the proposed method is evaluated in terms of the metrics such as total accuracy, false positive rate and detection rates. Comparing the logistic regression solution with existing methods, revealed results better than any of the current models in place.

Simulation study of application layer DDoS attack is performed by Bhandari, et al. (2015). The impact of Web Service Application layer DDoS attacks is determined by using NS2 Simulator for a web cache model. These web attacks are launched on the server capacity to handle requests and to determine if any legitimate users would get impacted in receiving the required web application services. Transaction throughput, successful HTTP transactions, server queue utilization by legitimate users, transactions drops and Transaction survival ratio metrics are calculated to measure the impact of the attack.

The summary of Cloud DDoS Attack References as stated in the review literature is illustrated in Table 2.2 below for the research papers reviewed from the year 2010 to 2016 regarding the Detection Techniques, Location and the level of DDoS attack.

Year	Reference	Detection Type	Deployed at	DDoS level
2010	Lo et al.	Signature	Access point	Infrastructure
	Bakshi et al.	Signature	Access point	Infrastructure
2011	Kim et al.	Hybrid	Access point	Infrastructure
	Kwon et al.	Anomaly	Access point	Not defined
	Gul et al.	Signature	Access point	Not defined
2012	Karnwal et al	Signature	Distributed	Application
	Bedi et al.	Anomaly	Access point	Not defined
	Chatterjee et al.	Hybrid	Access point	Not defined
	Chonka et al.	Hybrid	Access point	Not defined
	Modi et al.	Hybrid	Access point	Not defined
2013	Lonea et al.	Anomaly	Access point	Infrastructure
	Karnwal et al.	Signature	Distributed	Application
	Gupta et al.	Signature	Access point	Infrastructure
	Modi et al.	Hybrid	Access point	Not defined
	Zakarya et al.	Anomaly	Access point	Not defined
	Huang et al.	Anomaly	Access point	Infrastructure
	Lonea et al.	Signature	Access point	Infrastructure
	Choi et al.	Anomaly	Access point	Infrastructure
	Ismail et al.	Anomaly	Access point	Not defined
	Dou et al.	Anomaly	Access point	Not defined
	Negi et al	Anomaly	Access point	Not defined
	Jeyanthi et al	Signature	Access point	Not defined
	Gupta et al	Hybrid	Distributed	Not defined
2014	Zareapoor et al.	Signature	Access point	Infrastructure
	Vissers et al.	Signature	Access point	Infrastructure
	Choi et al	Signature	Distributed	Infrastructure
	Iyengar et al	Signature	Distributed	Not defined
	Michelin et al	Signature	Access point	Application
	Teng et al	Signature	Access point	Infrastructure
2015	Gamble et al.	Signature	Access point	Infrastructure
	Girma et al	Signature	Distributed	Not defined
	Wang et al	Signature	Access point	Not defined
	Marnerides et al	Signature	Access point	Infrastructure
	Chen et al.	Signature	Access point	Application
2016	Seyyed et al.	Hybrid	Access point	Infrastructure
	Selvaraj et al.	Signature	Access point	Application
	Wang et al.	Hybrid	Access point	Infrastructure

Table 2.2: Summary of DDoS Attack Mechanism

From the table summary the most common deployment location for DDoS defense tends to be the access point while the DDoS attack level is primarily aimed at Infrastructure levels.

2.4 DDoS ATTACK CLASSIFICATION

In order to understand the DDoS attacks better, attack types are classified as per degree and level of Attack Automation, Vulnerabilities Exploited, Attack Rate Dynamics and Attack Impact as shown in Figure 2.2 and presented in the section below.

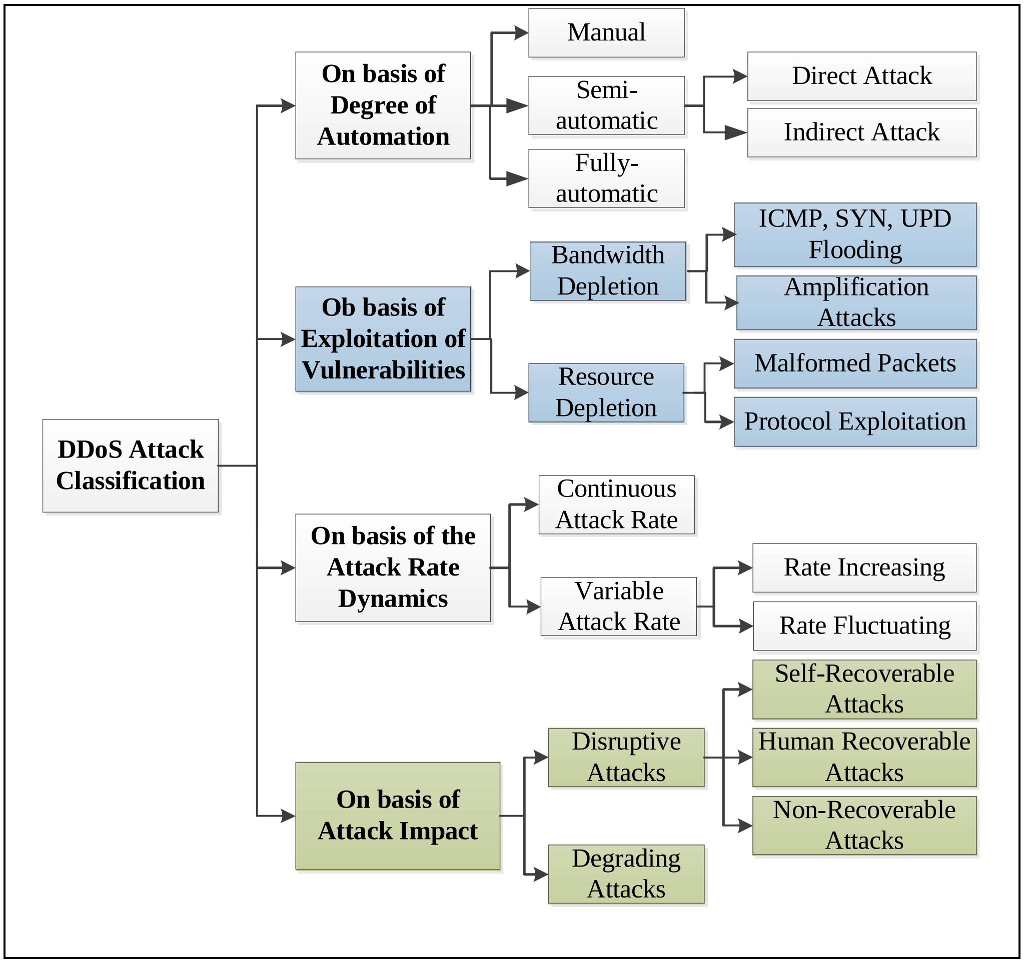

Figure 2.2: DDoS Attack Classification

- As per Degree of Attack Automation, manual attacks involve the attacker scanning the network, IP Addresses, machines for vulnerabilities, break into the system and deploy a code and executes a malicious payload for remote control access of that user system. The system is then kept ready to launch an attack on the attackers command. Semi-automatic attacks involve deploying attack scripts that scan and compromise the user machines and download a payload and installing the attack codes. These victim system are bots under control of the handlers who choose when and how about the attack type and target victims. Automatic attacks on the other hand are carried with a high degree of automation, with the compromised user systems having the attack code and software with predetermined type of attack, duration, victim's IP address. There is minimal interaction once the payload gets deployed or during the automatic attack.

- As per Exploitation of Vulnerabilities, Bandwidth Depletion attacks involve flooding and amplification clogging the WAN pipes with attack network packets. Flooding involves bots and zombies sending huge volumes of traffic to clog and congest the target's bandwidth pipes. The response from the victim slows down with the increase in such flood requests, saturating the bandwidth pipe, preventing access to the authorized users. Amplification attacks involve the bots and zombies sending messages to the target's subnet by broadcast. Resource Depletion attacks involve use of malformed data packets having incorrect IP packets being sent by the zombies with the malicious intent to crash it and protocol exploits which involve exploitation of a specific protocol feature to have the victim consume resources and ultimately make it unavailable to the legitimate users.

- As per Attack Rate Dynamics, continuous and variable rate DDoS attacks are most common. Continuous rate attacks are executed without break or lowering the force of attack. This leads to the disruption in services quickly; however, this attack gets detected as well. Variable rate attacks vary the attack frequency and force, carefully avoiding detection which ranges from having the attack increase in force or have a fluctuating rate of attack.

- As per the impact of the attacks, disruptive and degrading are two common types of attack. The impact of disruptive attacks is complete shutdown and leads to full denial of services to the legitimate clients. Recovery from such disruptive attacks has the impact based on automated self-healing recovery, Human intervention or is non-recoverable. Degrading attacks consume the victim resource bit by bit in small portions. This is much smarter than other attacks, making the attack difficult to detect.

2.5 PARAMETERS FOR Effective DDoS DETECTION

After reviewing the above mentioned research manuscripts for DDoS attack issues and classification attacks, the following parameters are identified for determining an effective DDoS detection mechanism.

- Real time Response Detection for real time, high speed, immediate or proactive response mechanisms for Advanced Application Attacks and Cloud Diversion attacks that have the ability to reduce the attack surface for say routing inbound traffic or have network ACLs that create stateless allow-and-deny rules in case of attacks are definitely effective as compared to reactive detection mechanisms

- Auto Scaling ability is the dynamic, scalability mechanism to handle flood attack, scale up bandwidth, utilize elastic load balancing for better fault tolerance during the attacks

- Throughput is the end to end time taken for the request generated by a legitimate clients for the server. The ability to sustain high levels of throughput determines the DDoS effectiveness.

- Request Response Time relates to the average time for a successful HTTP response. With the increase in attack rate, processing capability impacts the request response.

- Zero Day Attack Detection is being able to detect new, unknown vulnerabilities as well as detect attacks ranging from Netflow, Headerless Layer7 packet, Open Flow, Software Defined Networking (SDN) as shown by Qiao, et al. (2016) to feeds with other vendor signals.

- Performance Degradation rate is calculated from resource crunch of CPU cycles, Memory, Storage or network bandwidth.

- Accuracy of Defense Mechanism is a critical parameter to judge the detection mechanism regards to Sensitivity (True Positive or True Negative ratio), Reliability (False Positive or False Negative ratio) for the desired outcomes.

- Over-Under Mitigate detection effectiveness is also measured on the vendor's ability to mitigate as per Rate-Only, HTTP Server based Redirects, SSL Protections, Routing Techniques, Heuristic Behavior, JavaScript Challenge Response and Signature

2.6 DDoS COUNTERMEASURE TAXANOMY

While a number of research proposals and partial DDoS mitigation solutions are discussed above, most of these only assist in preventing very few aspects of the full DDoS attack. There seems to be no one shot comprehensive countermeasure against each known DoS attack. Every day, cyber attackers are coming up with new vector threats and attack derivatives in their attempts to bypass existing and new countermeasures deployed. This leads to the conclusion that more research is required when trying to design and develop an effective DDoS countermeasure solution. Taking into account the parameters in DDoS attack detection, the defense mitigation mechanisms are evaluated on a scale of 1 (Low) to 10 (High) in Table 2.3 below.

Attack Detection Parameters	**Centralized**			**Distributed**
	Source Based	**Destination**	**Network based**	**Hybrid**
Accuracy	3	9	3	5
Scalability	3	4	6	6
Performance	6	7	6	5
Complexity	2	3	7	6
Overall defense	No	No	No	Yes

Table 2.3: Comparing DDoS Mitigation Defense Mechanisms

The ideal time to mitigate a DDoS attack is right at the launching location of the attack by not allowing it to reach the target or even travel over WAN circuits. Achieving this is far from implementation. Classification, analysis and comparison of DDoS tools is performed by the Researcher for a better understanding of the existing tools, methods and attack mechanism along with a study of DDoS tools. This will provide a better understanding of DDoS tools in present times. From the observations of the review, most of the researchers carried out research on Infrastructure level DDoS attacks primarily due to the ease with which the Infrastructure attacks for network and application floods can be performed.

In Infrastructure level attacks, there is no exploitation of vulnerability, the attackers flood the bandwidth pipes with malicious traffic and consume computing resources, denying legitimate access to authenticated users. Application attacks on the other hand, exploit system and web application vulnerabilities at Application Layer 7 mimicking human behavior related to system weakness, outdated patches and misconfigurations while carrying out the attack.

CHAPTER SUMMARY

This chapter provides a survey of the DDoS attacks, taxonomy and parameters to mitigate the attacks. A comprehensive mitigation defense solution involves detection, blocking and mitigation of the DDoS flood attacks in real time and right at the initial DDoS attack source. For this the DDoS nodes need to be spread across the Internet globally. These nodes are used for the DDoS attack detection, response and prevention. Apart from this feature, the below mentioned factors should also be considered for the proposed DDoS attack mitigation solution.

- Functionality – be able to reduce if not block the impact of the DDoS attack, no matter how large or powerful the DDoS flood attack is.
- Ease of implementation – does not require any network design modification or infrastructure data flow reconfiguration
- Low overhead – should not pose additional overhead on the existing data center systems and processing power.
- Recognize Legitimate traffic – should not be reporting large number of false positives where in legitimate traffic is getting dropped during a DDoS blocking process.

The next chapter presents the cyber-attack trends and the results of the survey conducted by the Researcher in order to gain first hand insight into the cyber-attack threats and issues. The chapter reviews mitigating strategies for DDoS attacks and also reviews the existing distributed denial of service attacks mitigation solutions available currently in form of On Premise, ISP based and Scrubbing options.