1. **Mahwish collabs**
2. **Discuss three cloud features that are proven helpful to DDoS attackers**
   * Pay as you go
   * Auto Scaling
   * Resource pooling and elasticity
   * On demand services

Cloud computing provides an on-demand utility computing model where resources are available on “pay-as-you-go” basis. In particular, the cloud provider is an “Infrastructure as a Service (IaaS)” provider, who provisions VMs on-demand. On the other hand, a service provider is a cloud consumer who has placed the web service in the form of a VM (say an e-commerce application) in the infrastructure cloud provided by the cloud provider. Depicts a typical cloud computing environment with a large number of servers running VMs.

2.1. DDoS attack and cloud features

DDoS attacks have recently been very successful on cloud computing, where the attackers exploit the “pay-as-you-go” model [8]. There are three important features which are the major reasons behind the success trends of cloud computing. On the other hand, the same set of features is proven to be very helpful to DDoS attackers in getting success in the attacks (discussed in Section 2.2) We now discuss these three features in detail:

2.1.1. Auto scaling

Hardware virtualization provides a feature to shrink-expand resources of a VM while it is running. These properties permit the allocation of additional CPUs, main memory, storage and network bandwidth to a VM when required. Additionally, this can also be used to remove some of the allocated resources when they are idle or not needed. Multiple providers use this resource allocation mechanism with the help of auto scaling [16] web services, which allows cloud consumers to decide the resource need on the basis of resource utilization or similar matrices. The same feature is extended towards adding more VM instances on more physical servers and stopping when there is no need. Machine level scaling (vertical scaling) and data center or cloud level scaling (horizontal scaling) are two crucial features of utility computing. Scalability is achieved by spreading an application over multiple physical servers in the cloud. Scalability is driven by high speed interconnects and high speed as well as ample storage. Virtualization of operating systems plays an important role while considering the scalability of VMs. VM cloning and its subsequent deployment are quite fast. Hence, whenever there is a requirement, cloned VMs can be booted on other servers and used to share the load. Scalability is also strongly supported by the live migration of VMs, where a running virtual server can be migrated to another bigger physical server without almost no downtime offering uninterrupted scalable operation.

2.1.2. Pay-as-you-go

On-demand utility model has become very attractive for consumers due to its leaner resource accounting and billing model. “Pay-as-you-go” model allows a cloud consumer to use resources without physically buying them. A VM owner may want to add or remove more resources on-the-fly as and when needed. Other benefits of using cloud platform offer better hardware utilization and no need of arrangements like power, space, cooling and maintenance. Pricing or accounting plays an important role while understanding DDoS attacks in the cloud. Mostly, cloud instances are charged on an hourly basis and thus the minimum accounting period is an hour. Resources can be allotted on fixed basis, pay-as-you-go basis and by auctions. Similarly, storage and network bandwidth are measured using total size and total data (in and out) transfer. It is very clear that these models are “pay-as-you-go” models and are still evolving.

2.1.3. Multi-tenancy

Multi-tenancy gives the benefit of running more than one VMs from different VM owners on a single physical server. Multi-tenancy is a way to achieve higher hardware utilization and thus higher ROI (Return on Investment). An individual user may want to have more than one VMs running similar or different applications on a single physical server.

1. **Discuss the Economic aspects of the DDoS attack and its consequences on cloud resource allocation**
2. **Discuss the direct and indirect effects of attack on cloud**

We show directly visible attack effects as well as attack effects which are not directly visible or become visible post attack. Direct attack effects include service downtime, economic losses due to the downtime, auto-scaling driven resource/economic losses, business and revenue losses, and the downtime and related effects on services which are dependent on the victim service. There are a number of indirect effects to the cloud DDoS attacks. Attack mitigation costs, energy consumption costs, reputation and brand image losses, collateral damages to the cloud components and the effects due to recent smoke-screening attacks. Reputation and brand image losses may not be well quantified and may be treated as long-term losses [20]. Collateral damages include indirect DDoS attacks, addition migrations and scaling, and the energy consumption effects as given in [21]. We discuss all these attack effects in more detail in this section.

1. **Define smoke screening**

Attack based reflection and amplification are the new forms of the DDoS. There is an additional attack that is termed very dangerous, has been started showing its effect parallel to a DDoS attack. This attack is known as Smoke screening which is an attack to plan information or data breach behind a DDoS While DDoS distracts whole staff in mitigating or preventing from the present situation, the attacker may plan other attacks to harm.

1. **Define botnet**

Botnet attack are those in which the huge amount of victim machines that are using any kind of application having malware that is active at a time, attacker can control the device and at the same time there is an thousands of victim machine with different IP address are available for attack this is called botnet, a botnet controller directs a large number of automated malware driven bots to launch the attack.

1. **Discuss attack prevention techniques. Also discuss the strengths and limitation of each**

Attack prevention (P) DDoS prevention in the cloud is a pro-active measure, where suspected attackers’ requests are filtered or dropped before these requests start affecting the server. Prevention methods do not have any “presence of attack” state as such, which is usually available to the attack detection and mitigation methods. Therefore, prevention methods are applied to all users whether legitimate or illegitimate. Most of these methods are tested against their usability, which incurs an overhead for the server as well as legitimate clients. We further classify this direction in four subclasses:

1. Challenge Response.

2. Hidden Servers/ports

3. Restrictive Access

4. Resource Limit

|  |  |  |  |
| --- | --- | --- | --- |
|  | ***Subclasses*** | ***Strength*** | ***Limitation*** |
| 1. | Challenge Response | Effective and usable methods using puzzles to differentiate human and bots | Image segmentation, OCR, dictionary and parsing attacks, and puzzle accumulation attacks |
| 2. | Hidden Servers/Ports | Service is being offered to legitimate users while no direct connection is established with the real server in the first instance | Overhead of additional security layer and redirections |
| 3. | Restrictive Access | Admission control or instead of blocking/dropping responses are prioritized for different classes of users | Not scalable in case of massive DDoS with spoofing by large number of sources |
| 4. | Resource Limits | Limiting the economic losses by restricting the maximum usable resources by a VM | It does not prevent DDoS and its effects, except limiting the economic losses due to cloud billing |

1. **Discuss attack detection techniques. Also discuss the strengths and limitation of each**

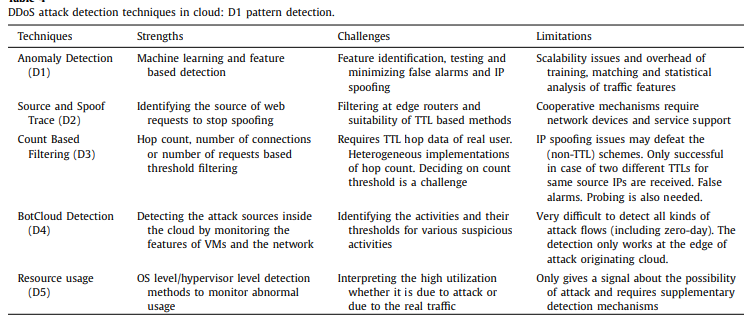
Attack detection is achieved in a situation where attack signs are present on the server in terms of its services and monitored performance metrics. These attack signs are initial signs, where the attack has just started to take the shape, or there may be a situation, where the attack has already deteriorated the performance. These methods may seem to be similar to “attack prevention” at times, and many of contributions have provided solutions in the same manner. Various performance metrics, which are monitored and affected due to an attack range from large response times and timeouts to higher memory and CPU usage. We further classify this section into five subcategories:

1. Anomaly Detection.

2. Source and Spoof Trace.

3. Count Based Filtering.   
4. BotCloud Detection.

5. Resource Usage.



1. **What are the drawbacks of using Resource Scaling as attack mitigation technique**

**Resource Scaling**

Dynamic auto-scaling of resources is one of the most popular features of the clouds. It is also treated as one of best mitigation methods to counter DDoS attack allowing server availability or continuity with scaled resources. Auto scaling can be done horizontally, where new instances may be started on the same or different physical server to serve incoming requests till the victim server is facing the attack. In vertical scaling, resources like CPU, memory and disk can be scaled in the same VM or the same logical unit. These extra resources can help the victim machine to.

1. Waste of resources
2. Waste of power consumption
3. Other VM on the same machine will suffer
4. False alarms may lead to EDoS. Co-hosted VMs may also be affected