DDoS Protection and Security Assurance in Cloud

10

Gaurav Somani, Manoj Singh Gaur, and Dheeraj Sanghi

Abstract

DDoS attacks have become a big concern for enterprises in the era of Internet computing. DDoS attacks have gained large attention from the community due to numerous fatal incidents in the last one decade. In particular, incidents on cloud services and cloud infrastructures have triggered anticipations related to heavy, longer, and hazardous attacks in near future. Additionally, economic losses due to these attacks, have given rise to Economic Denial of Sustainability (EDoS) attacks that exploit the on-demand resource provisioning feature of cloud computing. As attack strikes a service hosted on a cloud platform, the resource bottleneck would occur. Consequently, the ambiguity and inability to differentiate between legitimate and attacker traffic would lead to acquiring or buying more and more resources on the go. These fake resource claims would lead to a heavy economic burden, unnecessary downtime, power consumption, and migrations. This chapter targets at detailing the insights into the DDoS and EDoS attacks in cloud computing. Additionally, this chapter provides a comprehensive sketch of the present state of the art, recent incidents, their impact, cloud pricing and accounting mechanism, and its readiness for these attacks.

G. Somani (✉)
Department of Computer Science and Engineering, Central University of Rajasthan, Ajmer, Rajasthan, India
e-mail: gaurav@curaj.ac.in

M.S. Gaur
Department of Computer Science and Engineering, Malaviya National Institute of Technology, Jaipur, India
e-mail: gaurms@mnit.ac.in

D. Sanghi
Computer Science and Engineering, Indian Institute of Technology, Kanpur, India
e-mail: dheeraj@iitk.ac.in

S.Y. Zhu et al. (eds.), *Guide to Security Assurance for Cloud Computing*,
Computer Communications and Networks, DOI 10.1007/978-3-319-25988-8_10

Through this chapter, we argue that the present solution stack is not sufficient enough to deter or defend DDoS attack on cloud services. The major emphasis of the proposed chapter would be towards security assurance, loss sharing, and providing a detailed guideline about the ideal solutions.

Keywords
Cloud computing • DDoS attacks • EDoS attacks • Attack mitigation • Security assurance

10.1 Introduction

Cloud computing, as an emerging technology paradigm, has changed the enterprise IT planning. Even government services and public utilities have shifted their IT implementations from traditional fixed on-site infrastructure to on-demand cloud computing infrastructure. Cloud computing provides many features including better resource utilization, pay-as-you-go accounting, on-demand resource allocation, no maintenance overhead, no depreciation of resources, fault tolerance, minimum downtime, and many such similar features. DDoS attacks have been proven fatal for many websites. Recently, this has attracted the security community to find solutions to detect, prevent, and mitigate the attack. Importantly, DDoS attackers have reportedly shifted their interest from the traditional web services and started targeting cloud-based web services. This is necessary due to two important reasons, one, large number of cloud-based services or their versions of popular services and, two, it is easy for attackers to achieve the goals of the attack, which have turned it into EDoS (Economic Denial of Sustainability) attack. DDoS in cloud is effective due to the on-demand availability of profound resources. Many recent incidents of DDoS in cloud have shown enormous costs resulted due to a DDoS attack on a cloud-based web service [41]. This chapter aims at providing a detailed discussion about the DDoS attack in cloud, their attack and threat model, characterization, modeling, and solutions. In order to motivate readers to the developments and open areas of research, a comprehensive survey space is also provided with effective solution guidelines in the form of security assurance.

10.2 DDoS in Cloud Computing

A typical DDoS scenario in cloud is as shown in Fig. 10.1. Cloud will typically have multiple high-capacity servers connected using a high-speed network. Each of these servers is virtualized using hypervisors or virtual machine monitors (VMM). Virtualization enables these servers to run multiple guest operating systems on top of the virtual machines. One of these VMs is the victim VM, which is running a web server which has been targeted by attackers. These attackers may range from a single node to a large network of nodes which are also termed as Bot-nets. Bot-nets and their availability as hired services have led a completely new dimension of DDoS

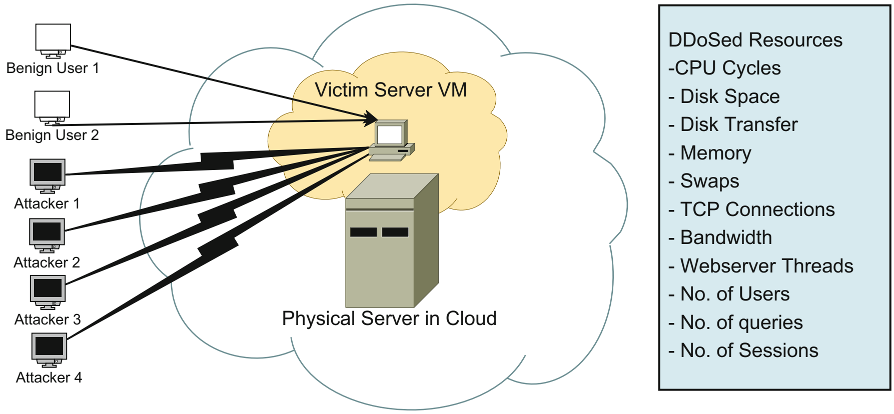

Fig. 10.1 DDoS scenario: cloud computing

attacks. Anybody having intentions to stop the web services of its competitors may hire services from a Bot-net provider on hourly basis and use thousands of nodes to flood the competitor servers. The attack packets may be of any type ranging from TCP SYN, ICMP, FTP or HTTP GET requests, etc. The aim of the attacker is to send more and more requests as to consume the usable resources on the server, in a manner such that the legitimate users would not get services with required quality or any service at all. Resources which may be exhausted by such requests may range from any of the resources listed in Fig. 10.1. Attackers may choose to exhaust one or more resources to get the desired success. Few of the resources are considered as easy resources to attack on, such as number of connections or sessions. If an attacker is successful in establishing the maximum connections, the server will not be able to serve legitimate clients anymore. The most important resource to consider from the perspective of cloud is CPU cycles. Attackers may plan to send a large number of requests in such a manner that the CPU utilization reaches the maximum (100 %), resulting in service denial. Now, let us take insight into cloud specifics which change the attack consequences differently. While the attack forces the virtualized server to reach maximum utilization of its resources, on-demand cloud which owns a huge amount of resources may add more resources to the virtualized server. This is because of the nature of the resource allocation and accounting models used in cloud. Cloud computing is a paradigm popularly known for the on-demand resource allocation and "pay-as-you-go" accounting model. In the absence of any DDoS protection mechanism, the cloud resource allocation algorithm would see a resource surge of victim server which is under attack. As per the allocation policy (usually termed as "auto-scaling"), cloud will automatically add resources to the victim server on the go. Theoretically, this may continue to large resource additions on regular intervals, in a hope that the increased resource utilization is due to the good users, e.g., flash sale on an e-commerce site. Inadvertently, this would enable the attackers to become successful in a fatal version of DDoS, EDoS, which is

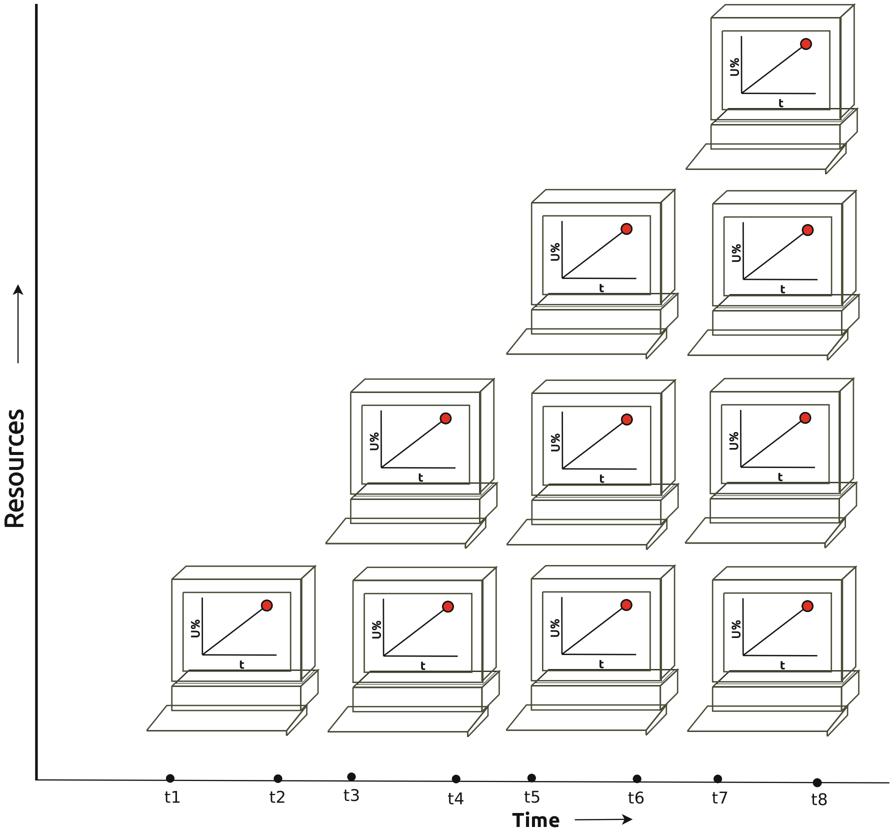

Fig. 10.2 DDoS in the form of EDoS in cloud

Economic Denial of Sustainability attack. This attack has attracted a large number of resource additions/buying from cloud, resulting into an enormous usage bill. There are instances where this attack has lead to thousands of dollars per hour to few popular services on Amazon EC2 Cloud. Though the shift of enterprises from fixed infrastructure on-site/hosted servers to on-demand remote cloud servers is happening for many good reasons, however, this has taken a shape of attackers' shift from fixed infrastructure servers to cloud-based servers. Behavior of cloud server and its allocation, in the presence of attack, is shown in Fig. 10.2. This figure shows a typical behavior, where a VM instance running in cloud is attacked by a DDoS attack at time $t1$. Due to the attack, the resource utilization starts rising, which, soon, results in to the maximum utilization of one or more resources of the VM. These resources may be any of the listed in Fig. 10.1. Generalizing the resource allocation strategies to the pure "on-demand" resource allocation, the auto-scaling feature of cloud would add more VM instances on the same or the other servers in cloud. In vertical scaling, the resource addition is done by adding more resources on the VM placed on the same physical server. In horizontal scaling, the resources are added in the form of additional VM instances on same or the other server in the cloud. Hybrid approaches can also be used having both vertical and horizontal scaling. As the attack continues with its request flood, more and more VM instances will be added and started to share the increased load. Based on the pricing and resource allocation model the consumer has opted, it will keep on adding resources, till it attains the maximum resources available or allowed based on the limits posed by the provider or consumer. Each time the resources (VM instances or resources) are added, the resource usage bill is increased. This resource bill may be enormous and as high as few thousand dollars per day [41]. After adding the maximum resources, the attack strength may result into the "service denial." Points between $t1$ and $t8$ show the attack consequences in cloud. This starts in the form of EDoS, continues as EDoS, and finally converges into DDoS. Economic harms are usually additional than the usual harms of DDoS attacks. The following are the major players, which either affects or gets affected in the whole DDoS scenarios [55]. This is very important for the aim of this chapter, as the security assurance is required to be adopted at each one of these players.

1. Victim server: This server is the direct victim of DDoS attack.
2. Attackers: One (DoS) or more nodes (DDoS) sending large number of requests. Spoofing may also be used.
3. Cloud as an entity: Cloud provider doing business by proving resources as a service.
4. Physical server hosting the victim server: This server is hosting multiple VMs in a multi-tenant environment. There is high possibility that this server will also be affected in addition to the cohosted VMs due to performance isolation aspects. Real resource demands will also be affected due to the fake allocation to the DDoSed VM.
5. Cohosted VMs: Mainly due to performance isolation aspects and unnecessary migrations/instance creation due to fake resource consumption by DDoSed VM which is subsequently into no resource availability.
6. Other physical servers: Other physical servers may be affected due to incoming migrated VMs and effects due to continuous DDoS attack.
7. Consumers to victim servers: Users of applications/services running on victim servers will be affected. The end users may be some other applications which are partially dependent upon the services of the victim web service. This results into business, rating, and reputation losses which are fatal for any organization.
8. Consumers to other VMs: Though indirectly affected, cohosted VMs user may also face service quality issues with the web service the victim web server is running.

Table 10.1 DDoS on fixed infrastructure vs. DDoS on cloud infrastructure

	DDoS on fixed infrastructure	DDoS on cloud infrastructure
Attack mechanism	Sending large number of requests by large number of nodes or Bot-nets	Similar to fixed infrastructure
Attack consequences	Service denial	Service degradation, economic losses due to resource buying and may finally result into service denial
Resource requirement at attacker side	Large	May even have effects on smaller number of resources
Effects on end users of the service under attack	Service denial	Service degradation and service denial on resource limit or exhaustion
Mitigation methods	Application layer or network layer mitigations	Additional mitigation required at cloud level or resource allocation level

10.2.1 History and Recent Incidents

DDoS attacks have been a center point of attraction in the security research and IT security planning for any enterprise. It is important to know and quantify the effects of DDoS on cloud infrastructures. DDoS attacks on fixed capacity (on-premise or hosted) are discussed. After that, recent DDoS attacks on cloud computing platforms are discussed to give an idea about their presence and nature. Table 10.1 shows the difference between "DDoS in Cloud" and "DDoS in fixed infrastructure." How the attack is being applied, its consequences, resource requirement while the attack occurs, and mitigation methods are the parameters, on which this comparison is made.

10.2.2 DDoS on Fixed Infrastructure

It is said that the first known DDoS attack was targeted to the University of Minnesota on their IRC servers in 1999 [20]. This attack had affected many machines in the campus and lasted for days. Similarly, Worldpay's payment and other services were affected by a DDoS attack in 2004, stopping its services which used to serve its clients spread to around 70 countries [44]. Subsequent to many of the similar attack incidents, various governments like the UK and Sweden had come up to legally ban DDoS attacks in 2006–2007 [35, 48]. The motives behind DDoS attacks have ranged from beating business competitions to political rivalry to cyber wars between countries. Massive DDoS attack was planned on Estonian websites in 2007 which resulted into a shutdown of major websites of the country [9]. A large DDoS attack had chocked the whole virtual gaming industry in Korea [4], costing it losses of more than $1 billion. Almost all the countries in the world have faced one or more similar attacks on their state infrastructures. Every country has large number of official websites which provide information and services for the public, defense services, intelligence services, and other information repositories for many other services. A large number of attacks have been reported on news websites [45, 58], e-commerce sites [59], and content provider websites [19].

10.2.3 DDoS on Cloud Infrastructure

DDoS attacks and their special version, EDoS, was first coined by Chris Hoff of Unisys in 2009. DDoS attacks in cloud are also termed as fraudulent resource consumption (FRC) attacks by Idziorek et al. in [22]. Authors have done characterization experiments to understand the impact of DDoS attacks on cloud infrastructure. Authors have shown that even sending mere 1 request/minute for a month from a single source results into an extra $2 bill on Amazon EC2 cloud. Authors have also calculated costs for heavy DDoS attacks where an attack of 5.2 Gbps would cost more than $6000 per day. This characterization can be extended and used for cost calculations with extensive usage of different resources. Looking at the recent attack in late 2014 and Q1 and Q2 of 2015, it is quite visible that cloud infrastructure-based services have become an easy target for DDoS attackers with effective results. A report by Alcatel-Lucent [42] signifies this argument by providing three important cases to this shift of attacker's mind. The first reported incident was on Sony and Microsoft gaming servers on Christmas day 2014. These servers provide popular gaming services for Xbox and playstation and were hosted on cloud servers. This gives a sign that multimedia and entertainment sites are among the favorites for a DDoS attack. Another attack targeted the cloud service provider Rackspace on its DNS services which disrupted the services around half of the day. Another notorious cloud-targeted DDoS was on Amazon EC2 servers, attacking it for on-line currency mining in 2014. This report had also highlighted the growth and possibilities to use cloud's profound and cheap resources in place of bots to plan DDoS attacks. In another report by Arbor Networks [43], there were attacks of the range of up to 154 Gbps in 2014 [6]. Similarly, the reports from Verisign [53] for Q1 of 2015 were threatening, as more than one third of the attacks mitigated by them were on cloud-based services/SaaS services. Reports in [47] have shown an attack cost rise of more than 400 % than the last year's data. This has been evident by the attack on GreatFire (www.greatfire.org), where the website faced a loss of more than $30 K/day on cloud-based operations [41]. There are multiple similar reports by industry which may be found out in [33, 46, 51, 57].

10.3 Attack Model and Threat Model

In this section, attack model and threat model for DDoS attacks in cloud computing platform are discussed. For better comprehension of these models, Tables 10.2 and 10.3 are given for attack model and threat model respectively. Attack model details about the features of a DDoS attack in cloud. On the other hand, threat model

Table 10.2 Attack model: DDoS in cloud

Features	Details
Attack packets	HTTP GET, TCP SYN, ICMP, HTTP POST, etc.
Attack frequency	Typically >500 requests/s, depends upon resources at both the ends [39]
Attack bandwidth	1–300 Gbps [6]
Typical attackers	A single source, a network, and bot-nets with or without spoofing
Attack methods	Low rate, flood, or flash mimic
Attack repetition	In many cases, repetition is done from different sources
Attack duration	Minutes to hours (average 72 min in [6])
Attack targets	Multimedia, government, e-commerce, cloud services, and many other targets
Attack motives	Competition, rivalry, cyber war between countries

Table 10.3 Threat model: DDoS in cloud

Threats to	Details
Victim server	Economic losses, service denial/downtime, unnecessary resource addition, VM instance creation, migrations, business and reputation losses
Cohosted VMs	Performance interference, resource race, and extra migrations due to resource exhaustion on physical server
Host physical server	Extra migrations and it would not be able to fulfill the requirements of cohosted VMs due to resource consumption by victim VM
Victim server owner	Downtime, economic losses, short-term and long-term business losses
Cloud provider	Extra migrations, performance interference to other VMs, large bandwidth bottleneck, downtime, and higher energy consumption
Other physical servers	Incoming migrations, VM instance creation, and consequent issues due to those VM instances under attack
Service end users	Poor service quality, downtime, and problems to other dependent services

illustrates various possible threats on attack targets and other elements and losses. Security literature uses both the models to provide better defensive solutions to various attacks. Though the literature uses both the terms interchangeably, however, here it would be better to comprehend in the present manner.

10.3.1 Attack Model

Based on the available literature [42] and recent incidents, it is clear that the attackers have shifted their attack targets from normal web services to cloud-based web services. This has resulted into happiness for cloud users that it will be easier to defeat the attack due to the availability of profound resources in cloud. On the other hand, attacker's joy cannot be ignored due to the easier- and difficult-to-detect

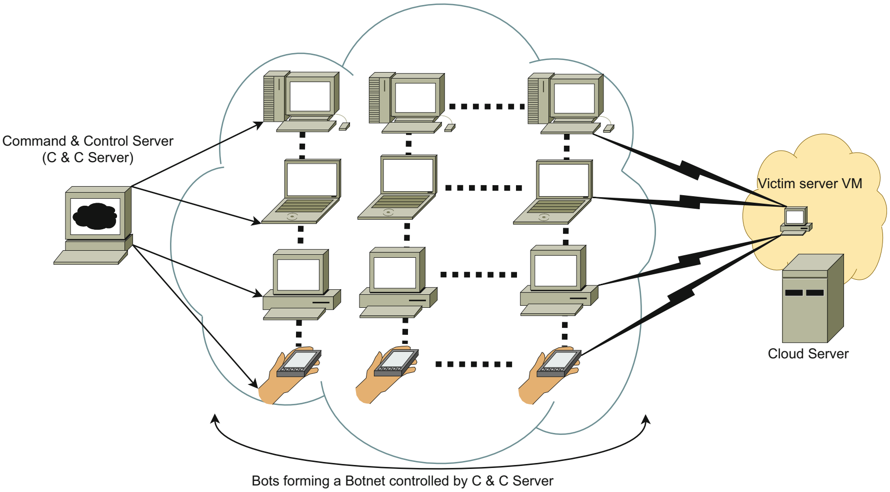

Fig. 10.3 Bot-net and C & C server

consequences of DDoS in the form of EDoS. Additionally, attackers may use cloud-based, profound resources-enabled bots to plan the attack [34]. It is important to note that the attack model is the same for both fixed infrastructure and cloud infrastructure. This is one interesting point to note that the methods of attack remains the same, while at the same time, the security community is required to spend efforts on devising new methods to circumvent and mitigate the attack in cloud platform as the consequences of the attack are different. "Bots on rent" has become quite a business these days, and there are multiple fatal stories in the recent past. Bots are typical malware programs, unknowingly installed by machines while on Internet. These bots are then controlled and used by Command & Control (C & C) servers to plan an attack (Fig. 10.3). There are reported incidents where the number of bots even ranged between 10,000 and 30,000 in number [26, 49]. These services are available on hourly basis charges on per hundred/thousand nodes. As success of DDoS attacks depends upon winning the "arms race," which is basically the resource race between attackers and victim servers, attackers are getting large number of cheap attack resources in the form of bots, while, on the other hand, victim server has dedicated resources on cloud to fight with the attackers. Bandwidth is the most important and costly resource these days, however, attacks consuming enormous bandwidth up to 300 Gbps have been observed in recent past. These sort of attacks change the whole scenario as they will consume and stress almost all the costly resources listed in Sect. 10.2. Attack duration is the most important factor while planning the mitigation. There are attack instances which last many hours to some lasting only few seconds. Average duration of these attacks have increased to 72 min from 60 min in 2014 [6].

10.3.2 Threat Model

Threat model gives the picture of how a variety of DDoS attacks result into various threats to different targets and stakeholders of cloud. In addition to service denial possibilities, economic sustainability issues are also important to ponder. Economic losses are mostly due to incorrect decisions made by on-demand resource allocation in cloud, which is also termed as "auto-scaling" (discussed in Sect. 10.2). These decisions are due to the resource utilization surge which results into the resource/VM instance addition which involves a cost. Performance isolation is one of the desired features of virtualization. However, performance interference and resource contention is still an issue in multi-tenant cloud. According to a detailed experimental and simulations study conducted by authors in [55], performance isolation and resource contention have been shown while DDoS attack is occurring on a cloud platform. In addition to losses to victim server, most of the other stakeholders in cloud environment are also affected. These indirect effects on nontargets are considerable in heavy attack DDoS scenarios. Stakeholders with various possible threat or effects on them are listed in Table 10.3. It is important to note that most of these effects are not available in the case of DDoS attack in non-cloud environment, except the service denial effects. Increased number of migrations, performance interference, short-term business losses (monetary) and long-term losses (business value), and higher energy consumption are important consequences of DDoS attacks in cloud which are also bothering nontargets. Proper isolation and DDoS protection is needed for all the VMs in multi-tenant environment as they are indirectly affected. Additionally, these effects should account to all the loss calculations and its sharing among these stakeholders.

10.4 System Model

In order to understand the DDoS attack, its impact, and relationship with the cloud resource allocation methods, a system model is presented. For more details on these models, readers are advised to contributions in [63] and [55]. A cloud will have the following components which are important for our discussion. There will be n physical servers.

$$P_i, i = 1, 2, ...n \tag{10.1}$$

and m VMs,

$$V_j, j = 1, 2, ...m \tag{10.2}$$

For resource accounting and billing, the resource items with each one of the physical servers and VM would be the following. Here, CPUs (C), memory (M), disk space (D), and bandwidth (B) are represented.

$$P_{i1} = C_i, \qquad P_{i2} = M_i, \qquad P_{i3} = D_i \qquad P_{i4} = B_i \tag{10.3}$$

Similarly, a VM V_j will have

$$V_{j1} = C_j \qquad V_{j2} = M_j \qquad V_{j3} = D_j \qquad V_{j4} = B_j \tag{10.4}$$

Capacity of physical server would be

$$Cap(P_i) = (C_i, M_i, D_i, B_i) \tag{10.5}$$

Capacity of a VM would be

$$Cap(V_j) = (C_j, M_j, D_j, B_j) \tag{10.6}$$

Cloud provides a feature of on-demand resource addition. The additional resource requirement would be

$$Require(V_j) = (C'_j, M'_j, D'_j, B'_j) \tag{10.7}$$

Each physical server has a limit on number of VMs it can host (r VMs). From V_j, few VMs as set V_s, s=1, 2,...... r, can be hosted if on P_i,

$$Cap(P_i) \geq \sum_{s=1}^{r} Cap(V_s) \tag{10.8}$$

and following all should also hold.

$$C_i \geq \sum_{s=1}^{r} C_s \tag{10.9}$$

$$M_i \geq \sum_{s=1}^{r} M_s \tag{10.10}$$

$$D_i \geq \sum_{s=1}^{r} D_s \tag{10.11}$$

$$B_i \geq \sum_{s=1}^{r} B_s \tag{10.12}$$

After successful placement of VMs of subset V_s on P_i, the idle resources on the server would be

$$Idle(P_i) = Cap(P_i) - \sum_{s=1}^{r} Cap(V_s) \tag{10.13}$$

While a VM is facing a DDoS attacks, the resource requirements will increase. This will trigger the auto-scaling algorithm, and resource requirement will be met by available free resources (from Eq. 10.13) which is only possible if

$$Idle(P_i) \geq \sum_{s=1}^{r} Require(V_s) \tag{10.14}$$

If one or more of the four equations (Eqs. 10.9, 10.10, 10.11, and 10.12) does not hold for a VM, it would require the auto-scaling to either for VM migration to another physical server which has required resources available. Another option is horizontal scaling which would add another VM instance (of the VM under attack) on another physical server. This would lead to the scenario shown in Fig. 10.2. As DDoS will stress resources, the auto-scaling will be misused by it to harm the server economically.

10.5 DDoS Protection in Cloud

In the previous section, we have built a model which tries to comprehensively detail the requirements of a DDoS mitigation system. In this section, we shall focus on the state-of-the-art literature on DDoS mitigation in cloud computing. There are large numbers of surveys published in the area of traditional non-cloud infrastructures which provide methods to overcome DDoS attacks. Some of them are in [12,13,50]. Though very few DDoS mitigation methods prove to be fit for cloud, still, following are the three broad sets of solutions which will make us aware about the present state of the art in the cloud space.

10.5.1 DDoS Prevention Methods

As shown in Fig. 10.4, the entry level methods, where the user request first arrives, can be tested to prevent the DDoS attack to occur. Challenge-response protocols have been the core part of many solutions in the DDoS mitigation area. These tests allow the system to identify whether the requester is a bot or a normal human being. Generally, most of the solutions follow the Turing test approach to validate this. A simple text problem, graphical puzzle, or a game-based problem is used to allow user to prove whether it is a human being. These problems will be generated in such a manner that it would be difficult for an automated bot/machine to generate answers. There are large numbers of solutions which are partially or fully implemented on the fundamentals of Turing tests [1,3,40,40,62]. CAPTCHAs are one of the most popular implementation of this approach. In one of the initial solutions to EDoS, authors in [56] have provided a Turing test-based system, which is known as EDoS-Shield. This system only provides access to clients which pass the graphical Turing tests. Similarly, text-based puzzles have been used by [27] and [21]. In addition to the puzzles, sometimes, the system also

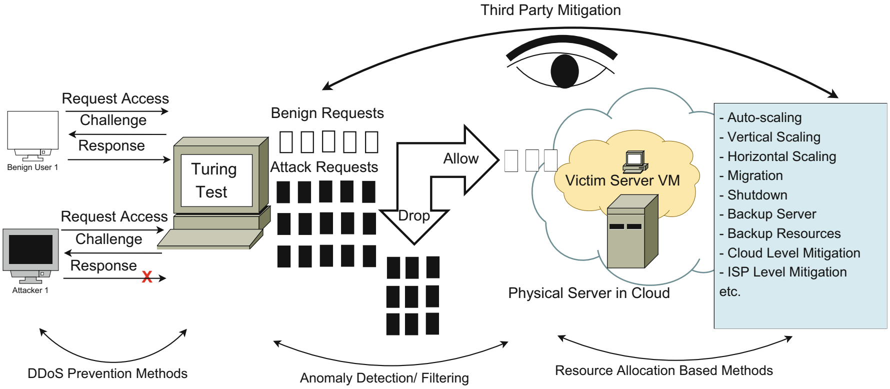

Fig. 10.4 DDoS protection in cloud at various levels

keeps a timer, in which the response should reach the server to stop computation of answers automatically. A different dimension to challenge response protocols is crypto puzzles, which are used to evaluate the compute power of clients. Many implementations have used them in [10, 28, 32]. At times, these puzzles have also been used as proof-of-work (PoW) approaches which shift the computation load on client and requires a response within a stipulated time to evaluate the capability of the clients. In addition to puzzle-based entry, there are approaches which have restrictive access policies. These policies take Turing tests as the first test, and after a suspected access, instead of dropping/blocking the requester, they would restrict for sometime/delay the requests [5, 28, 52]. Approaches exist which provide the access to "good" users on hidden servers or ports like hidden proxy servers in [61], ephemeral servers in [28], and hidden ports in [37]. In another approach, dynamic shuffling between clients and servers have been proposed to provide quality service to benign users [25]. Similarly, selective and goodwill-based access have been provided in the approached proposed by [28, 37].

10.5.2 Anomaly Detection

Anomaly detection is a major class of DDoS protection methods which are there to detect any anomaly pointing towards the occurrence of a DDoS attack. Many of these methods are based upon filtering the traffic on the basis of the phenomenon of natural traffic and its profile based on history. Time, frequency, access pattern, and count are few parameters which define the web behavior of a user which differentiates it from the other users. The second stage in Fig. 10.4 represents mitigations based upon these techniques. Techniques which are used in anomaly detection in fixed infrastructures have been listed in detail in [38]. The following are the four important categories of approaches which come under anomaly detection-based DDoS mitigation.

1. **Statistical pattern detection:** These approaches are based upon web access logs and features extracted from it. These features are compared with the features, and the deviation between them is used to detect the anomaly. Legitimate web requests have been modeled as "Zipf" distribution in [23], where authors have claimed to segregate good and bad traffic on the basis of the properties of distribution. Shamsolmoali et al. [54] have used a filtering method, which is based upon statistical filtering in which they have calculated the distance between profiles of good and bad traffic using Jensen-Shannon divergence [16]. Similarly, baseline profiling of TCP and IP flags have been used by [15].
2. **Threasholds** Thresholds or counts are quickest anomaly detection methods without much calculations. Number of requests in a specific period or request frequency is a common method to segregate traffic. This is mostly successful as the request count by a normal user can't match the frequency of attackers. Approaches in [24, 27, 52] used this method of anomaly detection. Similarly, hop-count-based filtering is used by [27] and [2] where the major assumption is towards IP spoofing. As per this assumption, the TTL or hop-count of spoofed IP addresses will be the same and can be used to detect the attackers.
3. **Sessions and Web Behavior** Time spent on a web page has been used as a metric in the contributions of [31], where authors have claimed that the attackers do not spend any time on the requested page. Similarly, Idziorek et al. [22] have proposed methods, where they could identify the web session from web logs. Differed sessions from the natural sessions would be filtered by the authors. Many approaches have used different ideas of web behavior of users in their detections. Authors in [7] and [11] have used the packet headers to identify the web behavior. Similarly, in [37], e-commerce website has been modeled for user behavior on various pages. Similar contributions exist in approaches [60], where authors have used HTTP and XML header in creating web behavior profiles.

10.5.3 Resource Allocation-Based Methods

As we have seen in the last two categories of DDoS mitigation systems, none of those methods target the cloud side of solution space. Additionally, most of those methods are similar to the ones which were there for detection in fixed infrastructure. In the system model, it has come up that the major emphasis of a mitigation solution should be towards minimizing the costs and resources. Following are some of the state-of-the-art approaches which have been proposed in the recent past after emergence of stable cloud services.

1. **Auto-scaling:** Auto-scaling being the core feature of cloud and major reason behind the success of DDoS in cloud requires major effort. Authors in [55] have proven the fatal behavior of auto-scaling approaches under attack. Methods are needed to be devised to have correct auto-scaling decisions under attack [36].
2. **Migration:** These methods are primarily used by horizontal scaling methods where the VM under attack is migrated from the bottleneck server to other

resourceful server. Many times, once the attack gets over, the VM under attack is again placed at its initial place. Authors in [64] and [34] have used backup servers and migration as their core approach while DDoS occurs.

3. **Resource usage-based detection:** The utilization matrices of VMs can be used to detect the possible attack scenarios. Virtual machine monitors can watch these activities and act accordingly. Authors in [64] and [34] used similar approaches. Shui et al. have used resource utilization of the servers in their mitigation methods.
4. **Backup servers and resources:** At the time of attack presence, some backup servers can be kept where the victim server can be migrated. Once the attack is mitigated or is over, the server can be placed back. Backup resources, their cost and migration costs are important factors to be considered while designing these methods. Authors in [63] and [34] have used this approach.
5. **Shutdown:** Shutdown of the server during the attack duration is another method to indirect mitigation but costs downtime. Shutdown-based ideas are used in [61].

10.6 DDoS Security Assurance in Cloud

This section includes the security assurance framework for DDoS attacks on cloud-based services. This framework is the gist of solutions available on each level of protection. Importantly, this framework also highlights the requirement to think in the direction of multilevel DDoS protection mechanisms as the traditional methods are not sufficient. Among the three categories of solutions presented in the previous section, most of the contributions concentrate on the solutions which work at the application layer or at the level of victim server. Research contribution like [55] and [63] have also argued to work at other levels of protection outside the victim server. A set of guidelines are provided with respect to each administrative or control level in Table 10.4.

1. **Victim level/application-level defense:** This is the level at which the server under attack has local control over application and its resources. This allows the application and the underlying middle ware and operating system to look at the

Table 10.4 Assurance at various levels

Assurance/defense level	DDoS assurance methods
Victim/application	Turing tests, Anomaly detection using web behavior and QoS monitoring, participation in auto-scaling
VMM	Resource usage-based detection
Cloud/network	Traffic monitoring, resource allocation pattern, resource limits (caps), migrations, attacks from cloud
ISP	Traffic segregation, ISP-level mitigations
Third party	Forwarding/intermediate server-based detection, cloud-based mitigation services, DDoS mitigation as a service

unusual patters in traffic, application usage and other locally available resource usage pattern. The minimum requirement for the prevention mechanism is a Turing test based on many of the challenge-response protocols. This allows the initial protection on the authentication-based websites. Even the first page, which is the home page of the website enabled with a Turing test, is prone to the DDoS attack. This requires efforts on the part of victim server to rely on other factors, like traffic patterns, transaction patterns, business value generation pattern, and the web behavior of users. This is important, in the sense that these patterns will get an insight into the real business or work the server is aiming to produce. The definition of work will always be different from application to application. This work may be a total number of buys or total sales amount for an e-commerce site, number of unique surveys filled on a survey site in some unit time.

2. **VMM/hypervisor-level defense:** Defense or detection at the level of hypervisor provides the additional outer view of the attack. After the victim server, hypervisor is the entity which can monitor the VM activities and provide necessary support for mitigation. This mitigation support requires additional information from application layer to understand whether the usage surge is due to an attack or there is really a great rewarding benign traffic which has come (which happens in the case of flash sales or large number of train reservations in the case of holidays or the visit at the FIFA site during tournament finals).
3. **Cloud-level/network-level defense:** Cloud-level defense can play a significant role in the case of DDoS. This is also important from the perspective of cloud as the mitigation service can be a part of cloud offerings which may attract service providers to choose the cloud. Additionally, at the level of cloud, it has full control of all the resources including the network resources, which help them to critically identify the overall resource usage, network traffic movement (inward and outward), energy consumption perspective, and migrations. These controls allow cloud to take abstract decisions to see any upcoming DDoS attack as well as resource requirement for genuine traffic. Accurate decisions can only be taken if there is a coordination between the three levels, victim, VMM, and cloud level. While we look for the industrial implementations at this level, Amazon has provided a feature to keep caps or resource limits on VMs. In addition to this, CloudWatch service [8] is provided to check and monitor many of the real-time accounting and resource usage information.
4. **ISP-level defense:** Internet service providers may also play a big role while mitigating the geographical DDoS attacks. These attacks may be originated from a specific organization or country pool and may target a similar group of servers from a different administration. ISP may collaborate and keep a high-level view of this unwanted flood and take necessary actions at networks level. Also this information in the form of alerts with attacker's information may help planning the clouds and victim servers. Solution on the similar lines are discussed in [18].
5. **Third-Party Defense:** Third-party mitigation systems are mostly onsite- or cloud service-based mitigation systems. Many of them have used the name DDoS mitigation as a service (DaaS) in cloud [14, 29, 30]. Most of these

solutions provide services as an overlay service which forwards the requests once satisfied. Many service providers have solutions in this market space [43,51,57]. Additionally, there are hybrid implementation in [17] which helps local firewall to mitigate the attack using profound cloud resources.

10.7 Chapter Summary

This chapter is aimed at providing a detailed tutorial cum open research direction guide for security enthusiasts working in the area of cloud security. Among many of the security issues studied by the community in the area of cloud computing, DDoS attack is proven to be the most fatal attack. This chapter has shown through recent incidents and cloud features that the effects of DDoS attacks are not on the same lines as it was with the traditional fixed infrastructure. A comparison of DDoS attacks, their effects, solutions, and major features have been compared between DDoS in fixed infrastructure and cloud infrastructure. A detailed and point-to-point attack model is presented to help readers understand the unique features of DDoS attack in cloud computing. The interesting part of the attack model is in its details which help the reader to understand the threat models. Threat models generally help in characterizing the effects of attacks with specific losses made by them to all the stakeholders. An effort has been made to prepare a threat model listing all the stakeholders and the impact of DDoS on them in addition to the real target. This is interesting to note that many of these stakeholders are significantly affected by the attack though not targeted directly.

A theoretical system model is also presented in the chapter detailing the cloud infrastructure, physical servers, virtual servers, and individual resources. Requirements of a good DDoS mitigation system have been established using the system model in addition to the important aspects. DDoS protections are surveyed and comprehensively discussed in three major categories including the most popular solutions. DDoS security assurance solutions at each level has been summarized in a manner such that to give detailed ideas to upcoming solutions in the space. DDoS attacks, their characterization, and mitigation solutions have become a vibrant area in the security space with large demands for solutions. This chapter has highlighted many of the open research problems in the space and possible solution pointers to readers.

10.8 Review Questions

1. What are the major differences between DDoS and EDoS attacks? Highlight the differences from the perspective of how the attack is planned and its consequences.
2. What are the important factors, which are considered by attackers to plan a quick and effective DDoS attack, without investing much of the resources?

3. What are the important effects of DDoS attacks to cloud and other stakeholders? Why the consequences are different as compared to traditional fixed infrastructures?
4. What are the attack and threat models of DDoS attacks in cloud infrastructures? Detail them.
5. What is the role of ISPs in mitigation of DDoS attacks? Discuss a typical example case of ISP role in DDoS Mitigation.
6. How DDoS security assurance can be guaranteed at various levels of mitigation?
7. How can a multilevel and multipoint mitigation system help in designing better solutions to defend against DDoS attacks?
8. Resource allocation in cloud is termed as a major cause for success of DDoS attacks in cloud. Why and how?

References

1. Abliz M, Znati T (2009) A guided tour puzzle for denial of service prevention. In: Annual computer security applications conference (ACSAC '09), Honolulu, pp 279–288, Dec 2009
2. Al-Haidari F, Sqalli MH, Salah K (2012) Enhanced EDoS-shield for mitigating EDoS attacks originating from spoofed IP addresses. In: Min G, Wu Y, (Chris) Liu L, Jin X, Jarvis SA, Yassin Al-Dubai A (eds) 11th IEEE international conference on trust, security and privacy in computing and communications (TrustCom 2012), Liverpool, 25–27 June 2012, pp 1167–1174. IEEE Computer Society
3. Alosaimi W, Al-Begain K (2013) An enhanced economical denial of sustainability mitigation system for the cloud. In: NGMAST, Prague, pp 19–25. IEEE
4. Arakaki T (2007) Dos attack cripples $1 billion virtual games trade – blackmailers blamed. http://texyt.com/dos+attack+hack+cripples+online+games+item+trade+00119
5. Baig ZA, Binbeshr F (2013) Controlled virtual resource access to mitigate economic denial of sustainability (edos) attacks against cloud infrastructures. In: Proceedings of the 2013 international conference on cloud computing and big data (CLOUDCOM-ASIA '13), Washington, DC, pp 346–353. IEEE Computer Society
6. Burt C (2014) Large volume ddos attacks see exceptional growth in first half of 2014: Arbor networks. http://www.thewhir.com/web-hosting-news/large-volume-ddos-attacks-see-exceptional-growth-first-half-2014-arbor-networks
7. Chen Q, Lin W, Dou W, Yu S (2011) Cbf: a packet filtering method for ddos attack defense in cloud environment. In: IEEE ninth international conference on dependable, autonomic and secure computing (DASC), Sydney, pp 427–434. IEEE
8. Amazon CloudWatch (2014) Amazon cloudwatch. https://aws.amazon.com/cloudwatch/
9. Davis J (2007) Hackers take down the most wired country in europe. http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all
10. Dean D, Stubblefield A (2001) Using client puzzles to protect tls. In: USENIX security symposium, Washington, DC, vol 42
11. Dou W, Chen Q, Chen J (2013) A confidence-based filtering method for ddos attack defense in cloud environment. Future Gener Comput Syst 29(7):1838–1850
12. Douligeris C, Mitrokotsa A (2004) {DDoS} attacks and defense mechanisms: classification and state-of-the-art. Comput Netw 44(5):643–666
13. See refrence [12]
14. Du P, Nakao A (2010) Ddos defense as a network service. In: Network operations and management symposium (NOMS), Osaka, pp 894–897. IEEE
15. Ismail MN, et al. (2013) Detecting flooding based doS attack in cloud computing environment using covariance matrix approach. In: ICUIMC, Kota Kinabalu, p 36. ACM

16. Gómez-Lopera JF, Martínez-Aroza J, Robles-Pérez AM, Román-Roldán R (2000) An analysis of edge detection by using the jensen-shannon divergence. J Math Imaging Vis 13(1):35–56
17. Guenane F, Nogueira M, Pujolle G (2014) Reducing ddos attacks impact using a hybrid cloud-based firewalling architecture. In: Global information infrastructure and networking symposium (GIIS 2014), Montreal, pp 1–6. IEEE
18. Gupta BB, Misra M, Joshi RC (2012) An ISP level solution to combat ddos attacks using combined statistical based approach. CoRR, abs/1203.2400
19. Hendrickson M (2008) Slideshare slammed with ddos attacks from china. http://techcrunch.com/2008/04/23/slideshare-slammed-with-ddos-attacks-from-china/
20. Hoffman S (2013) Ddos: a brief history. https://blog.fortinet.com/post/ddos-a-brief-history
21. Huang VS, Huang R, Chiang M (2013) A ddos mitigation system with multi-stage detection and text-based turing testing in cloud computing. In: 2013 27th international conference on advanced information networking and applications workshops (WAINA), Barcelona, pp 655–662. IEEE
22. Idziorek J, Tannian M Exploiting cloud utility models for profit and ruin. In: Proceedings of the IEEE international conference on cloud computing (4th IEEE CLOUD'11), Washington, DC, pp 33–40, July 2011. IEEE Computer Society
23. Idziorek J, Tannian M, Jacobson D (2011) Detecting fraudulent use of cloud resources. In: Proceedings of the 3rd ACM workshop on cloud computing security, Chicago, pp 61–72. ACM
24. Jeyanthi N, Mogankumar PC (2014) A virtual firewall mechanism using army nodes to protect cloud infrastructure from ddos attacks. Cybern Inf Technol 14(3):71–85
25. Jia Q, Wang H, Fleck D, Li F, Stavrou A, Powell W (2014) Catch me if you can: a cloud-enabled ddos defense. In: 44th annual IEEE/IFIP international conference on dependable systems and networks (DSN), Atlanta, pp 264–275. IEEE
26. Kandula S, Katabi D, Jacob M, Berger A (2005) Botz-4-sale: surviving organized DDoS attacks that mimic flash crowds (awarded best student paper). In: NSDI, Boston. USENIX
27. Karnwal T, Sivakumar T, Aghila G (2012) A comber approach to protect cloud computing against xml ddos and http ddos attack. In: 2012 IEEE students' conference on electrical, electronics and computer science (SCEECS), Bhopal, pp 1–5. IEEE
28. Khor SH, Nakao A (2009) spow: on-demand cloud-based eddos mitigation mechanism. In: HotDep (Fifth workshop on hot topics in system dependability), Estoril
29. Khor SH, Nakao A (2011) Daas: Ddos mitigation-as-a-service. In: 11th international symposium on applications and the internet (SAINT), Munich, pp 160–171. IEEE
30. Kim SH, Kim JH (2010) Method for detecting and preventing a ddos attack using cloud computing, and server, 12 July 2010. US Patent App. 13/386,516
31. Koduru A, Neelakantam T, Saira Bhanu SM (2013) Detection of economic denial of sustainability using time spent on a web page in cloud. In: 2013 IEEE international conference on cloud computing in emerging markets (CCEM), Bangalore, pp 1–4, Oct 2013
32. Kumar MN, Sujatha P, Kalva V, Nagori R, Katukojwala AK, Kumar M (2012) Mitigating economic denial of sustainability (edos) in cloud computing using in-cloud scrubber service. In: Proceedings of the 2012 fourth international conference on computational intelligence and communication networks (CICN '12), Washington, DC, pp 535–539. IEEE Computer Society
33. Labs K (2014) Global it security risks survey 2014–distributed denial of service (ddos) attacks. http://media.kaspersky.com/en/B2B-International-2014-Survey-DDoS-Summary-Report.pdf
34. Latanicki J, Massonet P, Naqvi S, Rochwerger B, Villari M (2010) Scalable cloud defenses for detection, analysis and mitigation of ddos attacks. In: Future internet assembly, Valencia, pp 127–137
35. Libbenga J (2007) Ddos attacks deemed illegal in sweden. http://www.theregister.co.uk/2007/02/20/ddos_attacks_illegal_in_sweden/
36. Mao M, Li J, Humphrey M (2010) Cloud auto-scaling with deadline and budget constraints. In: 2010 11th IEEE/ACM international conference on grid computing (GRID), Brussels, pp 41–48. IEEE

37. Masood M, Anwar Z, Raza SA, Hur MA (2013) Edos armor: a cost effective economic denial of sustainability attack mitigation framework for e-commerce applications in cloud environments. In: 2013 16th international multi topic conference (INMIC), Lahore, pp 37–42, Dec 2013
38. Mirkovic J, Reiher P (2004) A taxonomy of ddos attack and ddos defense mechanisms. SIGCOMM Comput Commun Rev 34(2):39–53
39. Moore D, Shannon C, Brown DJ, Voelker GM, Savage S (2006) Inferring internet denial-of-service activity. ACM Trans Comput Syst (TOCS) 24(2):115–139,
40. Morein WG, Stavrou A, Cook DL, Keromytis AD, Misra V, Rubenstein D (2003) Using graphic turing tests to counter automated ddos attacks against web servers. In: Proceedings of the 10th ACM conference on computer and communications security (CCS '03), New York, pp 8–19. ACM
41. Munson L (2015) Greatfire.org faces daily $30,000 bill from ddos attack. https://nakedsecurity.sophos.com/2015/03/20/greatfire-org-faces-daily-30000-bill-from-ddos-attack/
42. Nelson P (2015) Cybercriminals moving into cloud big time, report says. http://www.networkworld.com/article/2900125/malware-cybercrime/criminals-moving-into-cloud-big-time-says-report.html
43. Arbor Networks (2014) Understanding the nature of ddos attacks. http://www.arbornetworks.com/asert/2012/09/understanding-the-nature-of-ddos-attacks/
44. BBC News (2004) Worldpay struck by online attack. http://news.bbc.co.uk/2/hi/business/3713174.stm
45. CNN News (2008) Cnn web site targeted. http://edition.cnn.com/2008/TECH/04/18/cnn.websites/
46. Neustar News (2014) Neustar 2014 'ddos attacks and impact report' finds unpredictable ddos landscape. http://www.neustar.biz/about-us/news-room/press-releases/2014/neustar-2014-ddos-attacks-and-impact-report-finds-unpredictable-ddos-landscape#.U33B_nbzdsV
47. SPAMfighter News (2015) Survey – with ddos attacks companies lose around £100k/hr. http://www.spamfighter.com/News-19554-Survey-With-DDoS-Attacks-Companies-Lose-around-100kHr.htm
48. OUT-LAW.COM (2006) Uk bans denial of service attacks. http://www.theregister.co.uk/2006/11/12/uk_bans_denial_of_service_attacks/
49. Peng T, Leckie C, Ramamohanarao K (2007) Survey of network-based defense mechanisms countering the dos and ddos problems. ACM Comput Surv 39(1):3
50. See reference [49]
51. Prolexic (2014) http://www.prolexic.com/. http://www.prolexic.com/
52. Saini B, Somani G (2014) Index page based edos attacks in infrastructure cloud. In: Recent trends in computer networks and distributed systems security, Trivandrum, pp 382–395. Springer
53. Seals T (2015) Q1 2015 ddos attacks spike, targeting cloud. http://www.infosecurity-magazine.com/news/q1-2015-ddos-attacks-spike/
54. Shamsolmoali P, Zareapoor M (2014) Statistical-based filtering system against ddos attacks in cloud computing. In: 2014 international conference on advances in computing, communications and informatics (ICACCI), Delhi, pp 1234–1239. IEEE
55. Somani G, Gaur MS, Sanghi D (2015) Ddos/edos attack in cloud: affecting everyone out there! In: Proceedings of the 8th international conference on security of information and networks (SIN '15), New York. ACM
56. Sqalli MH, Al-Haidari F, Salah K (2011) EDoS-shield – a two-steps mitigation technique against EDoS attacks in cloud computing. In: UCC, Melbourne, pp 49–56. IEEE Computer Society
57. Technologies A (2013) Akamai's state of the internet q4 2013 executive summary volume 6 number 4. http://www.akamai.com/dl/akamai/akamai-soti-q413-exec-summary.pdf
58. Vamosi R (2008) Imdb victim of denial-of-service attack. http://www.cnet.com/news/imdb-victim-of-denial-of-service-attack/

59. Vance A (2005) Man admits to ebay ddos attack. http://www.theregister.co.uk/2005/12/28/ebay_bots_ddos/
60. Vissers T, Somasundaram TS, Pieters L, Govindarajan K, Hellinckx P (2014) Ddos defense system for web services in a cloud environment. Future Gener Comput Syst 37:37–45
61. Wang H, Jia Q, Fleck D, Powell W, Li F, Stavrou A (2014) A moving target ddos defense mechanism. Comput Commun 46:10–21
62. Yan J, El Ahmad AS (2009) Captcha security: a case study. IEEE Secur Priv 7(4):22–28
63. Yu S, Tian Y, Guo S, Wu D (2013) Can we beat ddos attacks in clouds? IEEE Trans Parallel Distrib Syst (99):1–1
64. Zhao S, Chen K, Zheng W (2009) Defend against denial of service attack with vmm. In: Eighth international conference on grid and cooperative computing, 2009 (GCC'09), Lanzhou, pp 91–96. IEEE

Gaurav Somani is an Assistant Professor at Department of Computer Science and Engineering, Central University of Rajasthan, India. He has completed his Bachelor of Engineering (BE) in Information Technology from University of Rajasthan with honors and Master of Technology (MTech) in Information and Communication Technology from DAIICT, Gandhinagar India, with distinction. He is pursuing his PhD from Malviya National Institute of Technology, Jaipur, India. His research interests include Distributes Systems and Security Engineering. He has authored a book/monograph on Scheduling and Isolation in Virtualization. He has published number of papers in various conferences and journals of international repute like ACM SINCONF, ACM CGC, IEEE CLOUD, and Elsevier FGCS. He has served as TPC member in multiple International conferences and reviewer of top journals like IEEE transactions on cloud computing. He is a member of IEEE and ACM.

Manoj Singh Gaur is Professor in the Department of Computer Science and Engineering at Malaviya National Institute of Technology Jaipur, India. He has obtained his Ph.D. from University and Southampton, UK. He has supervised research in the areas of Networks on Chip and Information Security. He has published over 150 papers in peer-reviewed reputed conferences and journals. He has coordinated national and international projects in the domains of Information Security and Networks on Chip. He is a member of IEEE and ACM.

Dheeraj Sanghi is a Professor of Computer Science and Engineering at IIT Kanpur. Since August 15, he has started working with IIIT Delhi. From 2008 to 2010, he served as the Director, LNM Institute of Information Technology (LNMIIT), a public-private partnership University in Jaipur. His research interests include network performance optimization, security, and distributed systems. He has visited about 70 colleges in India to discuss issues related to career planning, future of IT industry, curriculum, and various technical/research talks. He has published a large number of papers at reputed international conferences and journals. He regularly writes his popular ideas about higher education and learning on his blog, dsanghi.blogspot.com. Professor Sanghi has a B. Tech from IIT Kanpur and M. S. and Ph. D. from University of Maryland.