Computer Science Review 39 (2021) 100332

Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

Review article

Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions

Aanshi Bhardwaj [a,*], Veenu Mangat [a], Renu Vig [a], Subir Halder [b], Mauro Conti [b]

[a] *University Institute of Engineering and Technology (UIET), Panjab University, Chandigarh, India*
[b] *Department of Mathematics, University of Padua, Padua 35121, Italy*

ARTICLE INFO

Article history:
Received 11 August 2020
Received in revised form 23 November 2020
Accepted 27 November 2020
Available online 28 December 2020

Keywords:
Anomaly based detection
Cloud computing
DDoS attack
Economic denial of sustainability
Machine learning
Deep learning
Statistical methods

ABSTRACT

Cloud computing model provides on demand, elastic and fully managed computer system resources and services to organizations. However, attacks on cloud components can cause inestimable losses to cloud service providers and cloud users. One such category of attacks is the Distributed Denial of Service (DDoS), which can have serious consequences including impaired customer experience, service outage and in severe cases, complete shutdown and total economic unsustainability. Advances in Internet of Things (IoT) and network connectivity have inadvertently facilitated launch of DDoS attacks which have increased in volume, frequency and intensity. Recent DDoS attacks involving new attack vectors and strategies, have precipitated the need for this survey.

In this survey, we mainly focus on finding the gaps, as well as bridging those gaps between the future potential DDoS attacks and state-of-the-art scientific and commercial DDoS attack defending solutions. It seeks to highlight the need for a comprehensive detection approach by presenting the recent threat landscape and major cloud attack incidents, estimates of future DDoS, illustrative use cases, commercial DDoS solutions, and the laws governing DDoS attacks in different nations. An up-to-date survey of DDoS detection methods, particularly anomaly based detection, available research tools, platforms and datasets, has been given. This paper further explores the use of machine learning methods for detection of DDoS attacks and investigates features, strengths, weaknesses, tools, datasets, and evaluates results of the methods in the context of the cloud. A summary comparison of statistical, machine learning and hybrid methods has been brought forth based on detailed analysis. This paper is intended to serve as a ready reference for the research community to develop effective and innovative detection mechanisms for forthcoming DDoS attacks in the cloud environment. It will also sensitize cloud users and providers to the urgent need to invest in deployment of DDoS detection mechanisms to secure their assets.

Contents

[*] Corresponding author.
E-mail addresses: aanshibhardwaj@pu.ac.in (A. Bhardwaj), vmangat@pu.ac.in (V. Mangat), renuvig@hotmail.com (R. Vig), sub.halder@gmail.com (S. Halder), conti@math.unipd.it (M. Conti).

https://doi.org/10.1016/j.cosrev.2020.100332

1. Introduction

Cloud computing provides an on demand computing paradigm to access services, resources and applications over the Internet. It has led to a shift in functioning of IT companies by moving from self-deploying and running of their daily IT facilities to using cloud computing platforms for infrastructure, storage, and other services. The National Institute of Standards and Technology (NIST) enumerates five key attributes of cloud, viz. services provided on-demand, resource sharing, ubiquitous network access, quick elasticity and pay as you go service [1] , [2]. Despite numerous advantages, cloud platforms are vulnerable to various types of attacks, e.g., malware injection attack, Virtual Machine (VM) Escape, launch of malicious VM, DDoS, wrapping attack. DDoS is one of the most notorious attacks out of these cloud attacks, since it can cause service disruption, poor user experience, and severe economic losses leading to unsustainability, for businesses using cloud computing. In a DDoS attack, an attacker aims to deplete network infrastructure, capacity or compute resources by overwhelming it with requests. It compromises the cloud services and creates problem in responding to legitimate users. The main motivation behind DDoS attacks can be blackmail, demonstration of attack capabilities, vandalism, political disputes, hacktivism, business rivalry, distraction from exfiltration and other data theft activities.

A representative DDoS attack scenario is illustrated through Fig. 1 wherein different devices like mobile devices, IP cameras, Digital Video Recorders (DVRs), laptops, etc. are used to attack cloud infrastructure by turning the devices into bots. Bots are connected devices that have been compromised and are under the control of an external entity. The external entity, called the bot herder or command and control (C & C), directs these multiple bots to send an overwhelming number of attack packets to a critical cloud component, such as a victim server, leading to partial denial of service initially, and complete denial eventually.

DDoS attacks in traditional networks are distinct from DDoS attacks in cloud environment. This is because apart from DDoS attack effects like disruption of service, monetary loss caused by the downtime, negative impact on brand reputation, costs of mitigating attack, etc., there are additional attack consequences in the cloud such as extra economic costs incurred due to autoscaling, costs of the extra energy consumed, collateral damages to cloud computing elements, movement of data and services from one cloud environment to another, and the negative effects due to co-hosted VMs. DDoS in cloud leads to Economic Denial of Sustainability (EDoS) attack [3]. In an EDoS attack, attacker sends illegitimate traffic in an attempt to overburden the cloud resources which have been provisioned for the victim. This fraudulent usage leads to request for additional resources. Since cloud computing employs a usage based dynamic pricing model designed to add more virtual resources to maintain the defined QoS levels, the autoscaling leads to drastic increase in billing usage costs. As more and more resources get provisioned for the victim, eventually the increased billing costs lead to economic unsustainability for the victim. The pay-as-you-go and multitenancy features of the cloud further exacerbate how the DDoS attack will affect individual customers.

The main motivation for authoring this survey is the trend of increasing number of sophisticated DDoS attacks on cloud platforms in the last few years. According to [4], it has been expected that DDoS attacks will double to 14.5 million by 2022. A survey of security experts from France, Germany, Italy, Spain, UK and the US by the Neustar International Security Council (NISC) in January 2019 has revealed that DDoS attacks are perceived as the highest threat to organizations. As per a report by Verisign [5], the favourite targets of DDoS attacks are the organizations associated with Cloud/IT Services. DDoS detection and responding times are also increasing. A Cisco [6] report says that number of DDoS attacks more than 1 Gigabit per second (Gbps) will increase to 31.1 million by 2021. Imperva in 2019 has reported currently observing DDoS attacks over 500 Gbps once every week [7]. There is 217% increase in number of attacks detected in Q2 2020 than in the same period of 2019 by Kaspersky DDoS Protection services [8]. According to NetScout threat intelligence report in 2019, there was an astounding 8.4 million DDoS attacks. So, which means 670,000 attacks per month, 23,000 attacks per day, and 16 attacks every minute. Kaspersky's DDoS Q2 2019 report also mentions an increase of 18% in DDoS attacks in Q2 2019 as compared to Q2 2018 [9]. Keeping in view this unabating trend of DDoS attacks, it has become imperative for every organization to have an effective DDoS detection and mitigation strategy.

1.1. Related surveys

There are several other works in literature [10–20] which have highlighted the requirements of detection of DDoS attacks in cloud computing. In Table 1, we have summarized and shown the various aspects that distinguish our survey paper from existing

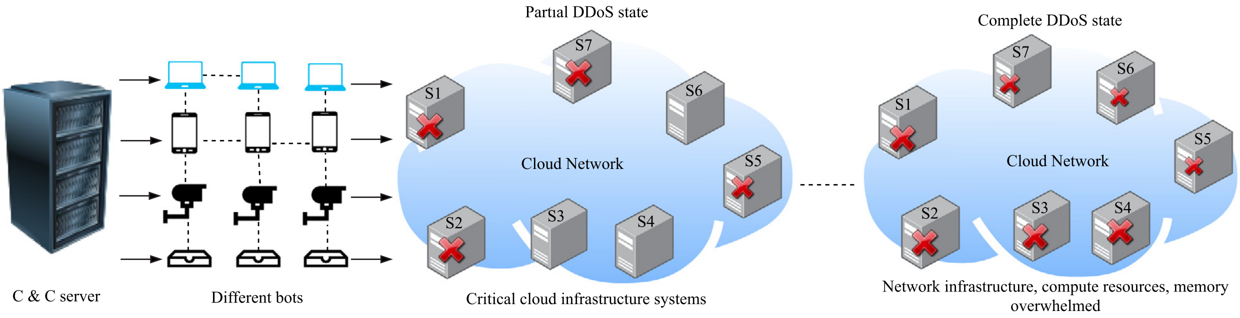
Partial DDoS state
Complete DDoS state
S7
S1
S6
S5
S2
S3
S4
Cloud Network
C & C server
Different bots
Critical cloud infrastructure systems
Network infrastructure, compute resources, memory overwhelmed

Fig. 1. Scenario of DDoS attacks in cloud.

related surveys. The columns indicate the major contributions of our survey work. A value of × indicates that the corresponding aspect (given in column) has not been dealt by the related survey (given in row), ∗ indicates that the aspect has been dealt with partially or not up-to-date, and ✓indicates that the aspect has been dealt comprehensively with sufficient level of detail and up-to-date. The last row refers to our survey paper.

Literature on DDoS attacks and mitigation strategies has been surveyed in [10]. Taxonomy of DDoS attacks and defence mechanisms has been presented for attacks done till Dec 2015. Categorization of DDoS attacks into infrastructural level and application level attacks has been done. Deploying anomaly based detection mechanism at access points has been proposed conceptually. Some detection methods that use statistical and machine learning approaches have been surveyed. In this paper, we attempt to identify more categories of cloud DDoS attacks based on recent attacks, and also provide a more comprehensive and detailed survey of anomaly based detection methods discussed in literature up to October 2020.

Authors of [11] have presented a detailed survey and taxonomy of solutions of DDoS attacks in cloud computing, and a comprehensive set of performance and evaluation metrics. They have proposed a systematic design of a defence solution involving five different levels of hierarchy viz. application level, VM/OS level, Hypervisor level, cloud level and ISP level. They have discussed specific features and aspects of the design at various levels. This survey paper is significantly different from [11], since it provides a current and comprehensive survey of anomaly detection, particularly detailed discussion of machine learning based anomaly detection methods. Additionally, this paper relates to several different aspects like attack incidents, commercial solutions and laws governing DDoS.

A survey and taxonomy of DoS and DDoS attacks, attacker and cloud security have been discussed [12]. Countermeasures have been explained with help of XML DoS and HTTP DoS. An overall defence strategy has been provided that includes detection, mitigation and security level architecture. It does not include detailed survey and discussion of detection techniques.

A survey and taxonomy of DoS and DDoS attacks in cloud environment has been presented [13]. Methods have been classified based on where detection mechanism is employed, viz. near source, near victim, intermediate, and when it is employed viz. before, during or after the attack. Information about various attack types, tools and datasets has also been given. There is limited discussion of DDoS attacks, no survey of anomaly detection techniques, and no discussion of statistical, machine learning and hybrid methods. Additionally, use cases, laws and commercial solutions of DDoS have not been mentioned.

The survey that has been presented in [14] discusses and provides a comparison of low rate, signature based, anomaly based, and EDoS defence mechanisms against different categories of DDoS attacks. It includes some work done up to 2016. As compared to this paper, [14] lacks discussion on cloud DDoS incidents, attack use cases, laws, commercial solutions, detailed discussion of machine learning methods, and comparison of machine learning, statistical and hybrid methods.

Various techniques to implement Intrusion Detection Systems (IDSs) such as signature based, anomaly based, Support Vector Machine (SVM) based, fuzzy logic, genetic algorithm, and Artificial Neural Network (ANN) based techniques have been discussed [15]. Host based, network based, distributed, and hypervisor based IDSs have been compared. Some DDoS detection techniques, up to 2016, have been listed along with dataset, evaluation parameters, advantages and disadvantages. There is no detailed discussion of detection using statistical and machine learning approaches, and no discussion of other facets of DDoS attacks.

A survey of application layer DDoS attacks and their prevention and detection mechanism has been presented in [16]. The surveyed detection mechanisms include those based on statistical measures like entropy, covariance; machine learning methods like Naive Bayes (NB), SVM, Decision Tree (DT); game theory; and chaos theory. They have discussed how a specific class of features like protocol features, system features, request features are suited for detection of a particular class of application layer attacks. The paper [16] deals with application layer attacks only and does not discuss recent DDoS incidents, types of DDoS attacks, laws, commercial solutions, taxonomy of anomaly detection and comparative analysis of statistical, machine learning and hybrid methods.

A tracing method for identifying threats in the cloud has been suggested [17]. Attacks in the cloud have been categorized using OWASP attack categories, mapped to threats using STRIDE threat model, and then mapped to components of cloud and their vulnerabilities. It has been concluded that more research is required to understand the new type of attack incidents to capture the threats that they pose. This paper is significantly different from [17] since it discusses DDoS attacks in detail with respect to cloud DDoS incidents, use cases, laws, commercial solutions, taxonomy and detailed discussion of anomaly based detection methods and subcategories.

Various mechanisms that can be implemented to prevent, detect and mitigate DDoS attacks in IoT have been surveyed [18]. Tools that can be used to form botnets and launch DDoS attacks, types of attacks in IoT, and defence mechanisms for IoT have been discussed. There is no insight on use cases, laws, commercial solutions, investigation of machine learning methods and comparison of statistical, machine learning and hybrid methods.

DDoS attacks and their defence in application, control and data plane of Software Defined Network (SDN) have been presented [19]. The architecture of SDN and cloud computing has been discussed. A brief overview of research work and open problems in the area has been given. Simulation tools for launching

Table 1
Comparison with related surveys.

Reference	DDoS incidents & patterns	DDoS use cases	Legal aspects	Commercial solutions	Taxonomy of DDoS	Taxonomy of anomaly detection	Machine learning aspects	Comparison of anomaly methods	Papers covered
Osanaiye et al. [10]	×	×	×	×	✓	✻	✻	×	2009–2015
Somani et al. [11]	×	✓	×	×	×	✓	×	×	2003–2016
Bonguet and Bellaiche [12]	×	×	×	×	✻	×	×	×	2006–2016
Gupta and Badve [13]	✻	✻	×	×	✻	×	×	×	2001–2016
Agrawal and Tapaswi [14]	×	×	×	×	✓	✻	×	×	2005–2016
Alzahrani et al. [15]	×	×	×	×	×	×	×	×	2008–2017
Praseed and Thilagam [16]	✻	✻	×	×	✻	×	✻	×	2003–2018
Hong et al. [17]	✻	✻	×	×	✻	×	×	×	2003–2018
Salim et al. [18]	✻	×	×	×	✓	✻	×	×	2004–2018
Dong et al. [19]	×	✻	×	×	✓	×	×	×	2001–2018
Singh and Behal [20]	✻	×	×	×	×	×	✻	×	2010–2020
Our Survey	✓	✓	✓	✓	✓	✓	✓	✓	2009–2020

✓— Detailed Study, ✻ — Limited Consideration, × — No Discussion.

DDoS in SDN and cloud have been listed. Our paper is significantly different from [19] as it discusses different aspects of DDoS in the cloud, namely, laws, commercial solutions, anomaly based detection, investigation of machine learning methods and comparison of statistical, machine learning and hybrid methods.

Authors in [20] reviewed DDoS detection and mitigation techniques in SDN. It discussed SDN architecture, various types of DDoS attacks in SDN and security challenges in SDN. It provided DDoS detection techniques on the basis of detection technique and metric used. They have not discussed DDoS use cases, its legal aspects, commercial solutions and taxonomy of DDoS attacks and detection techniques.

It is evident from Table 1 that this survey paper attempts to discuss DDoS in cloud computing with respect to fresh aspects and in a comprehensive and up-to-date manner. The increasing number of recent DDoS incidents with new attack vectors and strategies, have precipitated the need for authoring this survey paper. Our survey paper is intended to serve as a ready reference for the research community to develop effective and innovative detection mechanisms for future DDoS attacks in the cloud environment.

The scope of this survey paper is to present a holistic and current view of DDoS attacks in cloud environments and state-of-the-art scientific and commercial solutions for their detection. This includes presenting the recent threat landscape and major cloud attack incidents, inferences and patterns, taxonomy of cloud DDoS attacks, illustrative use cases, laws governing DDoS attacks, comparative listing of available commercial DDoS solutions, DDoS detection methods and their categories, comprehensive survey of literature on anomaly based detection, in-depth investigation of machine learning based detection, tools, platforms and datasets. To the best of our knowledge, no other survey paper provides complete and up-to-date information about all these facets of DDoS attacks in the cloud environment.

1.2. Contribution and organization of survey

This paper contributes to the field by providing a survey of state-of-the-art DDoS attacks as well as scientific and commercial solutions for their detection, which can be used in cloud environment. The major contributions of the paper are:

- Provides up-to-date listing of major attack incidents on cloud infrastructure while inferring how the trends in cloud DDoS attacks are evolving w.r.t. volume, intensity and frequency of various categories of DDoS attacks.
- Gives observations on upcoming DDoS attacks in future. DDoS attacks are expected to increase in intensity and frequency as more and more organizations move towards cloud platforms, adoption of IoT increases and DDoS-for-hire services become easily available. Multivector high volume attacks against single/multiple targets from numerous devices are expected to increase. New attack vectors and attacks perpetuated by nation states against critical infrastructure systems are expected.
- Enumerates alternative commercial DDoS solutions. A detailed listing of the major commercial DDoS detection solutions has been provided after studying the available products in the DDoS detection and mitigation market space.
- Presents a taxonomy of anomaly based DDoS detection methods. A detailed taxonomy of anomaly based DDoS detection methods has been presented. Based on recent research works that have been surveyed, new elements have been added to existing taxonomies.
- Explores the use of machine learning methods for detection of DDoS attacks and investigates their features, strengths and weaknesses, tools and datasets, and evaluates results of the methods.
- Presents comparative summary of statistical, machine learning and hybrid methods.
- Depicts sample illustrative DDoS attack scenarios. The first use case depicts disruption of healthcare services due to amplification attack, the second use case shows EDoS due to multivector attack, and the third use case depicts business loss due to stealthy attack.
- Discusses laws governing DDoS attacks in major nations.

The organization of the remainder of the paper is as follows. Section 2 provides an overview of the threat landscape and major cloud attack incidents from June 2014 to June 2020. Some inferences about the evolution of DDoS attacks in last 6 years and estimates of future attacks are presented. Section 3 discusses the categories of DDoS attacks in cloud and lists some observations and inferences regarding the nature of attacks. Section 4 presents a comparative listing of popular commercial DDoS solutions. Section 5 describes the DDoS detection process, taxonomy and survey of anomaly based methods, followed by an in depth discussion on statistical, machine learning and hybrid methods. It provides an investigation of machine learning methods based on features and datasets being used for training the models, platforms/ tools employed, strengths and weaknesses. A comparative summary of the categories of methods is also presented. Section 6 depicts three representative use cases for DDoS attacks and lists the laws governing DDoS in leading nations. Section 7 presents open research issues and gives recommendations for future work. Section 8 summarizes the observations and inferences regarding DDoS attacks and their detection in cloud environment.

2. Overview of threat landscape and attack incidents on cloud infrastructure

In this section, we present an overview of the threat landscape and major DDoS attack incidents on cloud infrastructure. In particular, we discuss major recent incidents of DDoS attacks (from June 2014 to 20) along with their impact in Section 2.1. A thorough study of these attack incidents has lead to observations about the nature of the attacks as well as few inferences about future attacks, which are stated in Section 2.2. Estimates for future DDoS attacks based on technical and research reports are presented in Section 2.3. This discussion highlights the recent trend of increasingly sophisticated DDoS attacks and emphasizes the need for conducting research to develop more effective DDoS detection and mitigation mechanisms.

2.1. Incidents of DDoS attacks in cloud

There has been a spate of DDoS attacks recently. Cloud anti-DDoS vendor Link11 in its report of DDoS statistics for Europe has registered 11,177 DDoS attacks on targets in Europe in Q1 2019. The number of hyper-scale attacks of over 80 Gbps has doubled in Q1 2019 compared to Q4 2018. The most common type of attack was using DNS reflection amplification vector in Q1 2019, followed by the Connectionless Lightweight Directory Access Protocol (CLDAP), which is used to increase bandwidth. Multi vector attacks increased to more than 46% with most attacks containing 2 or 3 vectors. The longest attack lasted 718 min. Peak attack bandwidth witnessed a 30% increase compared to Q4 2018 with values of 224 Gbps [21]. The main actors in the threat landscape are cyber terrorists, hackers, rival nation states, competing companies, naive customers and unwitting individuals.

Amazon Web Services (AWS) which provides on demand cloud computing services was hit by largest DDoS attack in 2020. It was a record breaking attack of 2.3 Tbps for almost three days. The biggest social media sites Facebook, Instagram and Whatsapp experienced issues globally with users being unable to access images and videos for 9–10 h on July 3, 2019. Whatsapp, Messenger and Instagram were also down for several hours on 12th March 2019. People around the world were not able to login to their accounts. Many network security experts confirm that outage was due to DDoS attack but Facebook denies it and claims that issues related to server configuration were the reason behind the outage. Two other major DDoS attacks occurred in April 2019 and Jan 2019 with attack sizes peaking at 580 million pps and 500 million pps respectively. These were successfully mitigated, albeit with a large cost. Attackers flooded the network with large and small SYN packets using botnets to generate an excessively large number of packets. A large number of attacks occurred in 2018 [22] and major ones are listed in the Table 2.

Another major DDoS attack was experienced at GitHub code hosting website on February 28, 2018 [23]. The peak attack size was recorded at 1.35 Tbps. The attack was a memcached amplification attack. Amplification attacks use a compromised server to redirect traffic to the attacked server. The size of the packet is increased by the amplification factor before being redirected to the attacked server. The amplification factor of various vectors are — NTP: 556.9, DNS: 179, and charge: 358.8. Memcached over UDP has a massive amplification factor of up to 51,000. On 21 October 2016, the most impactful and noteworthy DDoS attack was experienced at Dyn [24]. Due to this attack more than 60 large scale organizations like Spotify, CNN, Visa, Amazon, Netflix, Twitter etc. were taken down. The attack source was Mirai botnet which is a malware that finds unprotected IoT devices to infect them for launching DDoS attacks. Gartner forecasts that 14.2 billion connected IoT devices will be in use in 2019, and this number will increase to 25 billion by 2021 [25]. The IoT devices such as DVRs, CCTV cameras, baby monitors, smart appliances, Routers and Servers, can be easily be turned into bots. Various botnets available for launching DDoS are Wirex, Mirai, Sartori, Okiru, Masuta, Reaper, Omni, Jenx, Chalubo, etc. A new DDoS launch platform called 0x-booter which infects devices using a variant of Mirai called Bushido, surfaced in late 2018. There is a trend of newer Botnets, like DemonBot, which target Hadoop clusters. These Hadoop clusters are cloud integrated and connected to numerous IoT devices, which in turn, can significantly boost DDoS attacks in the cloud environment [26].

Table 2 presents the major DDoS incidents on cloud platforms in the last six years.

2.2. Observations and inferences

The recent DDoS attacks on cloud demonstrate a powerful increase in attacker's capabilities. A comparison of the recent severe DDoS attacks of 2019 (Jan and April) with the most severe DDoS attacks of 2018 (Feb and March) reveals some interesting points. The 2018 attacks that reached 1.7 Tbps and 1.35 Tbps were memcached amplification attacks. The generated attacks mainly consisted of large packets and a relatively low pps rate. The GitHub report confirms a peak of 129.6 million pps. These large packets had a single source port (port 11211) and originating service address on different servers. Therefore it is possible to mitigate these attacks by using a network mitigation appliance or mechanisms like Access Control Lists (ACLs) for traffic filtering. On the other hand, the DDoS attacks in 2019 were aimed at generating a large number of pps, up to 580 million pps, to exhaust the CPU and memory resources of servers, and to increase the mitigation cost of network hardware and other resources. Dyn attack in 2016 using Mirai was a multi vector high volume TCP and UDP flood and it generated compounded recursive DNS retry traffic. It involved at least 100,000 malicious end point devices. It was also aimed at throttling the bandwidth of the network. Mitigation efforts included traffic-shaping of incoming traffic, rebalancing of incoming traffic by modifying DNS querying anycast policies, application of internal filtering, and scrubbing. The attack vectors were known attack types, but the flexible DDoS generation system and segmented Command and Control which enables launching of simultaneous attacks against multiple targets, was the defining feature. This can have far-reaching consequences in a multitenant cloud system where VMs are co-hosted on same physical machine for different clients. It can be inferred that trends of DDoS attacks are evolving more towards increasing attack intensity, measured in pps, as well as increasing volume, as measured in bandwidth. The latter category, by itself, is relatively easier to mitigate.

2.3. Estimates for DDoS attacks

It has been more than 30 years since the first DDoS attack was witnessed. In 1988, Robert Morris wrote a self-replicating worm which quickly spread and consumed system resources. In September 1996, a DDoS attack occurred on New York's Internet Service Provider (ISP), Panix. The SYN flood based DDoS attack put the ISP offline for several days and affected 20 million users who were online at that time. Since then, several governments and nations, small and big commercial organizations, social organizations, banks, etc. have become targets of DDoS attacks, which have increased in size, frequency and complexity.

Table 2
Major DDoS incidents on cloud platforms.

Target	Attack date	Impact
European Bank [27]	June 21, 2020	Biggest pps DDoS attack of 809 million packets per second
AWS [28]	February, 2020	Largest DDoS attack till now of 2.3 Tbps
Wikipedia [29]	September 7, 2019	Site was unavailable in many parts of the world for around 3 days
Telegram [30]	June 12, 2019	Service disruption, user experience degradation
Electrical Grid in LA, Utah (U.S.) [31]	March 5, 2019	Interruptions in electrical grid operations
Imperva Client [7]	January 10, 2019	Service disruption, user experience degradation
Cambodia ISPs EZECOM, SINET, Telcotech, Digi [32]	November 2018	Sharp decrease in Internet speeds for over a week
Square Enix Co, Ubisoft [33]	October 4, 2018	Poor connections to games, increased server latency globally, online payments unavailable
ABN Amro and ING Dutch Banks [34]	May 24–25, 2018	Inaccessible online and mobile banking accounts, delayed response
Danish Railways [35]	May 13, 2018	App, ticket system and website crashed, email and phone lines disrupted
DNS Service Neustar [36]	March 2018	Broadcast storm leading to delayed response
Arbour Networks Client [37]	March 5, 2018	Delayed response
GitHub [23]	February 28, 2018	GitHub site blocked
Business Wire [38]	January 31, 2018	Huge delays in web service
ABN Amro, ING, RABO Banks and Dutch Revenue Office Online [39]	January 27–28, 2018	Online banking, websites and e-commerce payment platform unavailable
Electronic Health Systems, Latvia [40]	January 1, 2018	Inaccessible patient records, online prescriptions and medical certificate service halted
Crypto market IOTA [41]	January 2018	More than 3.94 million dollars stolen
DreamHost [42]	August 24, 2017	Disruption in hosting, locked virtual private servers, reduced email performance
Content Delivery Networks (CDNs)[43]	August 17, 2017	CDNs and content providers were down
Melbourne IT [44]	April 13, 2017	Disrupted web hosting, reduced email performance, blocked access to the Console
Imperva Incapsula Network [45]	December 21, 2016	Service degradation
Liberia Lonestar Cell MTN [46]	November 2016	Internet access crippled, huge revenue losses and high mitigation cost
Dynamic Network Services Company [24]	October 21, 2016	Amazon, Tumblr, Paypal, Netflix, Twitter unavailable
OVH Cloud Hosting [47]	September 2016	Hosting service down
KrebsOnSecurity website [48]	September 2016	Website down
BBC website [49]	December 31, 2015	BBC websites offline and unavailable
Ukraine Power Grid [50]	December 23, 2015	Power outages for about a quarter-million people for a period from 1 to 6 h
Linode [51]	December 25, 2015	DNS hosting outages, Linode Manager outages
Cloudflare CDN [52]	February 11, 2014	Unavailable servers, service disruption
Sony and Microsoft Gaming Servers [53]	December 25, 2014	Disrupted gaming service
Rackspace [54]	December 21, 2014	Increased latency, packet loss, connectivity failures
Codespace [55]	June 17, 2014	Data deletion

As per Corero [56], the average DDoS attack size will increase to 1 Gbps and number of DDoS attacks will grow to 17 million by 2020. The previous years did not experience too many high pps attacks as a large number of resources are required to generate effective attacks. But with the proliferation of IoT devices, most of which are unsecured, there is an increasing trend towards high intensity attacks. There is a trend towards multivector attacks launched through Botnets, like Mirai, Brickerbot, Reaper, etc. These attacks morph over time which makes detection and mitigation a difficult task. Attackers are using increasingly powerful botnets comprising misused cloud servers, hijacked IoT devices and embedded devices.

The popularity of DDoS for hire services or booters has increased. These services provide tools to malicious users for anonymously targeting anyone and can be availed by paying a nominal price. These services have been advertised on the dark web mostly, but recently hackers have started advertising them blatantly using social media. An example is the Cayosin botnet that has been advertised using YouTube and available on Instagram in February 2019. In April 2018, Europol cracked down webstresser.org service, which was the biggest market for hiring DDoS services. The service had around 150,000 users and was responsible for launching between four and six million attacks over the past three years. Security vendor Nexusguard has reported that booter websites more than doubled in Q1 2019 as compared to Q4 2018.

It has been predicted by Radware that the public cloud services market will grow by 17.3% to $206 billion by 2020 [57]. This shows that organizations are rapidly shifting to cloud platforms leading to more threats and vulnerabilities. This will make cloud platforms a major target for attackers. Attacks directed at nation-states, as well as perpetuated by them, are also expected to increase. This may be done by causing internet outages, service outages, supply chain attacks, healthcare systems attacks, etc. Attempted attacks against critical infrastructure networks are expected to increase.

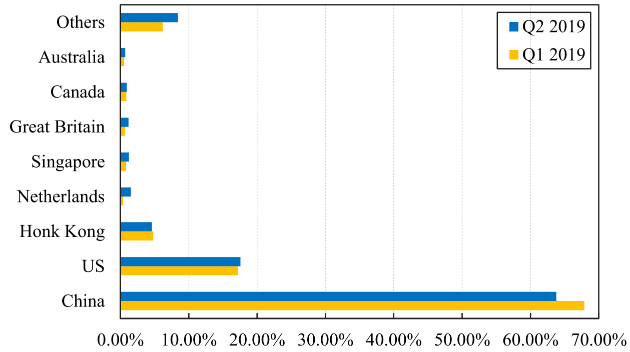

Fig. 2. Trends in geography of DDoS attack targets.

Fig. 2 shows distribution of DDoS attack victims country-wise in Q2 as compared to Q1 of 2019. China is the most targeted DDoS country even though there is a reduction in attack percentage from 67.89% to 63.80%. The percentage of attacks in US in Q2 2019 is almost the same as compared to Q1 2019, which is almost double of the statistics for US in Q4 2018. The figure also shows DDoS attack percentage for other countries like Netherlands, Australia, Canada, Hong Kong etc.

3. Categories of DDoS attacks

In this section, we provide a categorization of DDoS attacks from a cloud computing perspective. This examination is useful in order to appreciate how the various DDoS attacks can impact the cloud environment and to be able to design effective detection mechanisms for the same. The well known categories of DDoS attacks are mentioned first. This is followed by discussion on DDoS attacks by categorizing them based on which part of the cloud is attacked. Section 3.1 discusses DDoS attacks on cloud infrastructure components, Section 3.2 discusses attacks on cloud services, and Section 3.3 discusses attacks on cloud customers.

DDoS attacks can be targeted towards depleting bandwidth or depleting resources of a network or a combination of both these approaches. The categories of DDoS attacks are: volumetric (Gbps), protocol (pps) and application layer (rps) attacks. Volumetric attack or floods target the bandwidth of the network and can be launched through botnets or amplification. Protocol attacks target the compute and memory of servers and intermediate devices and often work at layers 3 and 4 of the OSI model on network devices like routers. Most attacks can be categorized depending on the vector and packet size, and the categories often overlap. Detailed description of DDoS volumetric and protocol attacks and their corresponding detection methods has been discussed in [58]. Application layer/layer 7 attacks are also viewed as a resource based attacks. These type of attacks target servers hosting some kind of a web application. The attackers in most cases make legitimate requests like a website user, and require very few bots to attack which makes it difficult to detect such type of attacks. As a consequence, these attacks displays much smaller traffic spikes. Application layer attacks are computed as requests per second (rps) or the number of requests made to an application. Detailed description of application layer attacks, and their corresponding detection methods has been discussed in [16].

DDoS attacks result in service disruption which is the primary effect. Service downtime/disruption leads to economic losses and short or long term business reputation losses. DDoS attacks in cloud might not always result in service downtime due to autoscalability feature of cloud. Autoscalability is one of the characteristics of cloud which automatically adds or removes computational resources based on usage at that instant. But it has the negative impact of increased billing costs for the cloud users. Additionally, since co-hosted VMs on a single physical server may be shared amongst different cloud users (multitenancy), there is collateral damage to non targets by disrupting their service and causing autoscaling of their resources as well. Fraudulent resource consumption results in economic losses to cloud users and reputation loss to cloud providers. Fig. 3 depicts the various DDoS attack categories from a cloud computing perspective. The attacker attacks different components of cloud according to the intent and existing vulnerability. The various cloud components that come under DDoS attacks are — Cloud Infrastructure (VMs, Hypervisor, Cloud Scheduler), Cloud Services (SAAS and web services) and Cloud Customers (Cost accountability component).

3.1. Attacks on cloud infrastructure

The attacks on cloud infrastructure are as follows:

Flooding Attacks: It is a denial of service attack in which a service is put down by overwhelming it with a large amount of traffic. The attacker floods the target with incomplete connections which consumes resources of target, and as a result, the genuine packets are not processed. Examples of flooding attacks are ICMP Flood, TCP SYN Flood, UDP Flood, ACK Fragmentation Flood, HTTP Flood.

Carpet Bombing: It is a new variant of common flooding or reflection attack. Instead of attacking a specific IP address, the attacker attacks multiple systems which are a part of subnet or CIDR blocks. Flooding CIDR blocks also overwhelms the mitigation system. The other issue is that detection systems usually rely on destination IPs but not on the subnets or CIDR blocks. This hinders the timely and accurate detection of attack.

Yo Yo Attack: This attack exploits autoscalability mechanism of cloud. The attacker sends periodic bursts of traffic which triggers the autoscaling process to alternate between scale up and scale down cycles. Rather than suffering from complete denial of service, the cloud users suffer from economic damage, i.e., the extra cost which has to be paid due to fraudulent packets causing the auto scaling process to scale up.

VM Sprawling: VM sprawling indicates the over abundance of resource draining VMs in the cloud environment, some of which may be obsolete. They are open to attack due to vulnerabilities that have not been patched up since the VM was last used.

Multi Vector: It is a new attack type in which the attacker combines different attack strategies to intensify the attack and make it difficult for systems to detect and mitigate the attack. The attacker may combine different types of flood attacks or may blend different amplification attacks or amplification attacks with traditional attacks.

Smurf & Fraggle: Smurf and Fraggle are amplification attacks. These attacks exploit the characteristics of broadcast networks. Smurf attack uses spoofed ICMP ping message to broadcast address, prompting each host to reply back, which further results in huge amount of traffic towards the victim. Similarly in Fraggle attack, the attacker sends spoofed UDP packets instead of ICMP packets.

CIDoS: Cloud Internal Denial of Service (CIDoS) attacks are those in which VMs attack their host with the help of covert channels. Each VM increases its resource consumption to disturb the host machine's ability to process the increase in resource usage. These attacks are harder to detect as the attack pattern is very similar to normal traffic.

3.2. Attacks on cloud services

The attacks on cloud web services and Software as a Service (SAAS) are as follows:

HTTP Flood: The attacker send legitimate HTTP GET or POST request towards the server. The attack GET and POST requests are similar to the normal HTTP requests. These volume of requests is so large that it consumes the resources of the target, leading to denial of service.

Billion Laughs: It is also known as XML bomb or exponential entity expansion attack. The attacker targets the XML parsers. The attacker may send a well formed XML message with schema validation which consumes the resources of cloud.

Cross Site Scripting: The attacker injects malicious JavaScript code into the targeted website. The code gets triggered when the user visits such websites. Upon execution of the code, the consumption of target resources jumps up, resulting in denial of the services running on the target.

Coercive Parsing: The attacker intentionally includes large number of namespace declarations, continuous open tags, deeply nested XML structures, which clogs up the CPU cycles.

NTP, Memcached DNS Amplification: NTP is a reflection based amplification attack in which the attacker exploits the functionality of NTP servers. The attacker sends spoofed requests towards the NTP servers which results in large response. Large number of such amplified responses consume the target resources, leading to denial of service. Similarly, in Domain Name Server (DNS) and Memcached amplification attacks, the attacker exploits DNS and Memcached servers for generating high volume and high bandwidth consuming DDoS attacks.

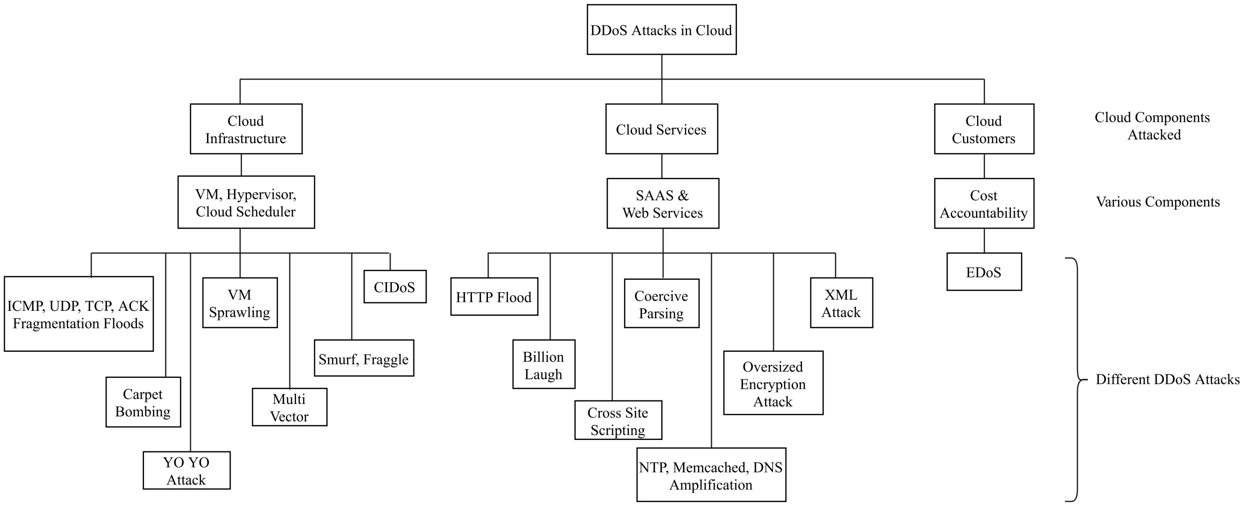

Fig. 3. Categories of DDoS attacks in cloud.

Oversized Encryption Attack: The attacker crafts the SOAP messages by including oversized digital signatures. These digital signatures when processed consume a lot of space in memory, leading to denial of service.
XML Attack: The attacker sends flood of XML messages towards the target. These messages are complex and parsing them is time consuming. The attacker manipulates some fields of XML message which eats up large resources of web services, ultimately breaking down the server.

3.3. Attacks on cloud customers

The primary attack that directly targets cloud customers is as follows:
Economic Denial of Sustainability (EDoS): DDoS attack is transformed to EDoS attack for cloud customers. The attack targets the economic resources of the customers by billing them for fraudulent resource consumption. The illegitimate usage of cloud resources is caused due to autoscaling of resources which has in turn arisen due to attack traffic, and not the customer's genuine traffic. This can lead to potentially infinite billing costs for the customer, leading to economic unsustainability for the cloud customer.

Inferences and Observations: At the network level, the most common attacks are TCP, UDP and ICMP floods, followed by reflective DNS, SNMP, SSDP floods. Fragmented packet attacks such as IP Fragment and TCP Segment are fairly common too. These attacks occur when reassembly of IP or TCP packet causes CPU saturation as packet is malformed with overlapping or missing values. They utilize very less bandwidth of attack/incoming traffic making them hard to detect. The common attacks at application layer are repetitive GET, low and slow attacks using Slowloris and its variants, slow read, and especially crafted stack/protocol/buffer attacks.

4. Ddos commercial solutions

In order to protect against the DDoS attacks (as discussed in Section 3), various vendors provide DDoS detection and mitigation solutions globally. This section begins by outlining the main requirements for a useful DDoS detection and mitigation solution, and then discusses popular commercial solutions, along with their strengths and weaknesses. This information is useful in determining the most suitable commercial alternative to defend an organization against DDoS attacks.

Various vendors provide DDoS detection and mitigation solutions globally claiming to keep operations of the client enterprise secure and available 24 × 7. The main design goals for a DDoS detection and mitigation solution are:

- Reliable and accurate detection of attack traffic
- Support for detecting multi-vector attacks
- Real time detection and mitigation of threats. Three time spans need to be minimized, viz. time from launch to detection, time from detection to redirection/mitigation, and time from detection to remediation
- Threat Intelligence
- Scalability to absorb volume of traffic as infrastructure and services grow
- Performance guarantee to keep up with rising attack volumes
- Web based GUI to give insight into the real-time traffic analysis, showing blocked DDoS attacks, server availability and providing metrics on current server response times
- Real-time monitoring dashboard to analyse applications, server behaviour and incoming and outgoing traffic
- Report generation of individual incidents and routine reports
- Cost-effective and easy integration with minimum extra hardware required and maximum Return on Investment (RoI)
- Availability

The popular vendors of anti-DDoS solutions and their products are discussed below. A listing of popular vendors and their product offerings is given in Table 3.

- **Akamai:** Kona Site Defender, Prolexic Solutions products protect websites and APIs against DDoS. They provide delivery through cloud and use automation in CDN-based and DNS components, and automated DDoS scrubbing. They are capable of dropping malicious network layer attacks at the edge. Product includes Web Application Firewall (WAF) and is scalable, supporting over 61 Tbps. Akamai DDoS pricing is single charge and does not charge extra based on size or frequency of attacks. Improvements can be made in WAF features and dashboard look and feel. It also needs more advanced application layer protection against SQL injection, applied scripting. Mostly used for securing financial services, commerce, broadcasting, publishing, public sector, high-tech, SaaS, manufacturing, healthcare, energy and gaming companies. Major clients are — Adobe, Airbnb, Cathay

Pacific, Benq, Fiat, Honda, Philips, Siemens, Verizon, Standard Chartered [59].

- **Amazon:** AWS Shield Standard provides protection from layer 3 and layer 4 DDoS attacks. AWS Shield Advanced includes intelligent real time detection and mitigation of application layer DDoS attacks like HTTP floods or DNS query floods as well. It provides DDoS cost protection and extensive visibility into attacks. It includes AWS WAF and is easy to setup. However, AWS Shield Advanced is expensive at $3000 a month, with additional data transfer usage costs. Major clients are — MedStar Health, MediData, Illumina, Philips, Practo, Nasdaq, Dow Jones, British Gas, Vodafone, Expedia [60].
- **Arbour DDoS:** Arbour Cloud, Arbour Edge Defence products provide on demand solution for low and high bandwidth DDoS with up to 7.6 Tbps scrubbing capacity. Arbour Edge blocks inbound and outbound malicious communication. It can act on volumetric, TCP, and application layer DDoS attacks. Arbour's Pravail Availability Protection System (APS) can specifically handle application-layer and TCP state-exhaustion attacks. Arbour products employ ATLAS global threat intelligence, and reputation data from Arbour Security Engineering and Response Team (ASERT). Delivery can be through on-premises appliance, VM, or AWS instance. It has a user friendly interface but is not backward compatible with routers that do not support NetFlow version. Also, it is expensive for small companies. It is used by enterprises, government, financial services and small and medium businesses (SMBs). Major clients are — iWeb, Frost and Sullivan, neoTelecom [61].
- **AT&T:** AT&T DDoS defence offers cloud-based monitoring of volumetric DDoS attacks, detailed traffic analysis for anomalies, packet scrubbing, web based GUI for status reporting, cloud signalling and automated mitigation of DDoS. It also analyses netflow to filter traffic. It is expensive to use this product with costs for mitigation going up to $3500 per month. Major clients are — Data Netw, State of Georgia, SMBs in healthcare and manufacturing industry [62].
- **CDN77:** CDN77 DDoS protection provides real time protection against volume based and protocol attacks. It is scalable with a large capacity network. It is primarily used for improving loading speed on websites. CDN77 is deployed successfully for website security and acceleration, live streaming, gaming, and private CDN. However, it may prove expensive for low use users. Major clients are — Oracle, Hubble Space Telescope, Bata, Avast, CentOS [63].
- **Checkpoint:** DDoS protector shields application infrastructure against known and unknown emerging security threats. It has four modules for security which are anti-DDoS, Intrusion Prevention system (IPS), SSL attack protection and network behavioural analysis (NBA). It provides vast range of mitigation and connectivity capacity. The bandwidth mitigation capacity ranges from 6 to 400 Gbps. Major clients are — SmartWave Technologies, PFNiG, Unitel, MTN etc. [64].
- **CloudFlare:** Argo tunnel protects web servers from direct attack and Cloudflare Spectrum gives protection for TCP and UDP service. These products automatically detect and mitigate layer 3, 4 and 7 DDoS attacks. These intelligent products automatically filter bad traffic by learning from past attack data. Delivery can be through cloud. Pricing is competitive. Basic product is free for personal websites, professional version is available for a fee of $20 per month per domain, and business version costs $200. New product launched in March 2019, CloudFlare Spectrum for UDP, provides DDoS protection and firewalling for unreliable protocols. The products can be improved by including more open APIs. Mostly used by software R&D companies. Major clients are — Nasdaq, Netwrk, Udacity, Discord, Mapbox, Zendesk, Quizlet, Digital Ocean [65].
- **Corero:** Smart Wall Threat Defence System (TDS) products detect large network layer, application layer, and reflective amplified spoofed DDoS attacks (including multivector and stealthy attacks). They utilize modern DDoS mitigation architecture to detect and filter DDoS attack traffic, while allowing legitimate traffic to flow uninterrupted. They can be deployed in various topologies like inline or scrubbing. They provide scalability with scrubbing capacity up to 4 Tbps and good visibility of the inbound and outbound traffic. Major clients are — Hyve, Streamline Servers, Liquid Web, htp GmbH, InMotion Hosting, TeleSystem, Jagex [66].
- **Fortinet:** Forti DDoS 1200B is a hardware based single solution for layer 3, 4 and 7 attacks that offers behaviour based anomaly detection with ultra low latency. FortiDDoS Cloud Monitoring service allows for visualization of attack impact and services availability. It is easy to deploy, and includes comprehensive analytical and reporting tools. The cost of base licence is around $ 4,050, in addition to the cost of the actual appliance. Major clients are — British Telecommunications, Chunghwa Telecom, Richter Gedeon, Tigo, EkoSistem [67].
- **Imperva:** Products Behemoth 2 and Imperva Incapsula name server offer website and infrastructure protection for Web, SSH, FTP, Telnet, SIP, SMTP, UDP, TCP, and DNS servers. They prevent direct-to-IP DDoS attacks by hiding the IP of origin server. A virtual firewall compatible with Microsoft Azure is included in product. There is easy integration with other devices. However, it is not possible to scale down and the cost may be too prohibitive for small companies. Business version costs $299 per site per month and professional version costs $59. Mostly used by enterprises and governments. Major clients are — eToro, NTT TechnoCross Corporation, NetRefer, PayMetric, Vietnamese Govt., Keysone RV Company [68].
- **Kaspersky:** Kaspersky DDOS protection defends against high-volume and complex attacks using special sensor software and advanced intelligence. It can be seamlessly integrated with no additional hardware required. Detailed post-attack analysis and reports are also provided. Major clients are — Ferrari, Mosgaz, Alfa-Bank, AZ-Sint Jan, Chemist Warehouse, Resolute Mining [69].
- **Link11:** DDoS protection Cloud offers protection against DDoS attacks on Layer 3, 4 and 7 based on self learning AI architecture. It employs fingerprint technology for intelligent threat detection. Product includes secure DNS, WAF and CDN. The pricing model is simple and allows for easy scaling. Major clients are — Hermes, German Federal Office of Criminal Investigation, CBC, top DAX companies [21].
- **Microsoft:** Azure DDoS Protection offers real time monitoring and automatic mitigation of DDoS threats. It uses adaptive tuning and integrates with Azure monitor for analytics. DDoS cost protection is another attractive feature. It is very easy to enable. However, protection cannot be tailored for individual resources. Basic protection is included with Azure service. Standard tier protection costs $2944, plus data charges for up to 100 resources. Major clients are — Telit, Clover Imaging group, Kodak Alaris, Mediterranean Shipping Company [70].
- **Sucuri:** Sucuri Firewall is a cloud based WAF that offers protection against layer 3, 4 and 7 attacks, and improved performance with its Anycast CDN. It uses machine learning to effectively detect DDoS attacks. It also offers unlimited

Table 3
DDoS commercial solutions.

Vendor	Product Name	Strengths	Weaknesses
Akamai [59]	Kona Site Defender, Prolexic Solutions	• Protects websites and API against DDoS • Drops network layer attacks at the edge • Includes WAF • Supports over 61 Tbps	• WAF features, dashboard look and feel can be improved • Needs more advanced application layer protection
Amazon [60]	AWS Shield	• Real time detection of application layer DDoS attacks like HTTP floods or DNS query floods • DDoS cost protection	• Cost of AWS Shield Advanced is prohibitive
Arbour DDoS [61]	Arbour Cloud, Arbour Edge Defence	• On demand solution for low and high bandwidth DDoS • Up to 7.6 Tbps scrubbing capacity • Arbour Edge blocks inbound and outbound malicious communication	• Not backward compatible with some routers • Expensive for small companies
AT&T [62]	AT&T DDoS Defence	• Cloud-based monitoring of volumetric DDoS attacks • Detailed traffic analysis for anomalies • Mitigation	• Very high mitigation costs
CDN77 [63]	CDN77 DDoS Protection	• Real time protection against volume based and protocol attacks • Large capacity network	• Expensive for low use users
Checkpoint [64]	DDoS Protector	• Does not block legitimate traffic • Reduced TCO of security management • Large number of security tools in one box • Single management application	• Expensive solution
CloudFlare [65]	Argo Tunnel, Cloudflare Spectrum	• Argo tunnel: protects web servers from direct attack • Cloudflare spectrum: Protection for TCP and UDP services • Competitive Pricing	• More open APIs should be provided
Corero [66]	Smart Wall Threat Defence System	• Detects large network layer, application layer, reflective amplified spoofed DDoS attacks • Scalable	• Pricing plans undisclosed
Fortinet [67]	Forti DDoS 1200B	• Hardware based single solution for layer 3, 4 and 7 attacks • Behaviour-based DDoS protection • FortiDDoS Cloud Monitoring service for visualization of attack impact and services availability • Easy to deploy	• Additional cost of hardware appliance
Imperva [68]	Behemoth 2; Imperva Incapsula Name server, website and infrastructure protection	• Protects Web, SSH, FTP, Telnet, SIP, SMTP, UDP, TCP, DNS servers	• Scaling down is not an option • Cost is prohibitive
Kaspersky [9]	Kaspersky DDOS Protection	• Protection from high-volume attacks • Seamless integration with no additional hardware • Special sensor software • Advanced intelligence • Post-attack analysis and reports	• Performance unknown against slow rate attacks • Pricing information is undisclosed
Link11 [21]	DDoS Protection Cloud	• Protection against DDoS attacks on Layer 3, 4 and 7 based on self learning AI architecture	• Pricing information is undisclosed
Microsoft [70]	Azure DDoS Protection	• Real time monitoring and automatic mitigation • Adaptive tuning • Integration with Azure monitor for analytics • DDoS cost protection	• Protection cannot be tailored for individual resources • Standard tier protection is expensive
Sucuri [71]	Sucuri Firewall	• Blocks layer 3, 4 and 7 attacks • Cost effective for websites	• Performance unknown against zero-day attacks
Verizon [72]	Verizon DDoS Shield	• Hosted, cloud-based DDoS protection • Intelligence driven security	• Interface is not very user friendly • Cost is high for small businesses

malware removal service. It is cost effective for securing websites with plans starting from $10/month. Major clients are — iThemes, GoDaddy, Yoast, Cart66, Softwear Systems, NYU, 24Digital [71].

- **Verizon:** Verizon DDoS Shield offers hosted, cloud-based DDoS protection and intelligence driven security. It provides hybrid DDoS mitigation by combining locally deployed mitigation appliances with a cloud-based mitigation service. Verizon product offers considerable capacity to withstand high volume attacks. Verizon offers flat monthly fees plan. The cost is unspecified, but known to be high for small businesses. Moreover, the interface is not too user friendly. Major clients are - U.S. military, utility companies, healthcare companies [72].

5. Detection of DDoS attacks

Having discussed the various types of DDoS attacks in Section 3 and anti-DDoS commercial solutions in Section 4, in this section, we elaborate the actual methods and techniques for detection of DDoS attacks based on a comprehensive survey of recent literature. Section 5.1 describes the three types of DDoS detection methods viz. signature, anomaly and hybrid detection. The rationale behind considering anomaly detection as the preferred method for thorough study, is then discussed in Section 5.2. A taxonomy of anomaly based DDoS detection methods is presented based on recent works in Section 5.3. This is followed by an in-depth investigation of each subcategory of anomaly detection method viz. statistical, machine learning, and hybrid method in Section 5.4. The critical analysis of literature on all subcategories of anomaly detection methods has revealed a comparison of these methods. This comparative summary is presented in Section 5.5. The cloud simulation-related framework and datasets that are used by researchers to conduct experimental investigation on DDoS detection mechanism in the cloud environment, are presented in Section 5.6. This section provides complete technical details to enable researchers to carry out experimental study of different DDoS detection mechanisms in the cloud environment.

Nowadays, IPv6 protocol has been adopted due to increase in number of IP addresses required by users. But due to security vulnerabilities in IPv6 protocol it can easily be exploited for launching DDoS attacks. A comprehensive survey discussing IPv6 based DDoS attack categories and defence solutions have been provided in [73].

5.1. Methods for detection of DDoS attacks

Classically, detection of DDoS attack can be categorized into three types: Signature based detection, Anomaly based detection and hybrid detection. Signature based detection technique uses a database of known attack rules. Traffic patterns are monitored for finding malicious events by comparing the patterns against the database. If the pattern is matched, the system raises alarm detecting attack. Signature based detection performs well in terms of detection accuracy if the database of rules is regularly updated. This technique fails to detect unknown attacks or zero-day attacks which leads to high false negatives. Maintaining an updated database of signatures is tedious and costly. The DDoS attacks employing botnets like leet and Mirai, are a prime example of cases where signature based detection methods are ineffective. These attack methods access local files and jumble or obfuscate their content to generate randomized payloads through millions of compromised devices. Since there is negligible similarity between packets, signature based methods are unable to detect an attack.

Anomaly detection refers to the identification of patterns that do not comply with expected behaviour [74]. The terms ‘anomalies’ and ‘outliers’ are most commonly used, sometimes also interchangeably, in the context of computer networks. Anomalies may be point, contextual or collective. The network administrator prepares a baseline profile by recognizing network behaviour during non-attack period. The main aim is to observe or find subsequent patterns that vary from baseline profile.

First, information of malicious and non-malicious traffic is collected and then it is sent to anomaly detection module for detection of attack. On detection of anomaly, alert command is issued to network operator which mitigates or fixes the attack. Hybrid based detection method is a combination of anomaly based and signature based detection methods.

5.2. Inferences and observations related to DDoS detection methods

The major advantages of employing anomaly detection techniques for DDoS attack detection in cloud environment are:

- Anomaly detection techniques can detect new or unusual behaviours in the traffic in a timely fashion. This can help prevent or, at the least, control the potential widespread impact in terms of economic loss, reputation loss, service disruption, from affecting the multitenant cloud users.
- Anomaly detection techniques lower the False Alarm Rate (FAR) for known and unknown or zero day attack.
- It is difficult for attackers to know what actions can be carried out without getting revealed since baseline profile of normal behaviour is unknown to them.
- Anomaly detection directly leads to outlier detection, wherein a flag is raised whenever a user or server or entity is acting significantly different from other entities of its type at a given time.

The major challenges in adoption of anomaly detection techniques for detection of DDoS attacks in cloud environment are:

- Given the large number and variety of users in a multicloud environment, it is very difficult to define a normal baseline profile that includes every possible normal behaviour. User behaviour analytics is needed. Furthermore, it is strenuous to set a precise demarcation between normal and abnormal behaviour. The demarcation is more of a hyperplane than a line. Additionally, it is difficult to detect an event or reading that is close to the boundary as normal or anomalous.
- Anomaly detection needs to consider the variations due to different time periods and trends in the baseline profile, which is defined in terms of parameters like throughput, web requests, user logins, etc., while setting threshold values. Manually configuring alerts for these fluctuating values is a challenging task.
- Most of the anomaly based approaches build or learn a normal traffic activity profile or model and detect network traffic that deviates from baseline profile as anomaly. Thus, they are able to detect new attacks that deviate from normal traffic. False alarms can be a challenge for these techniques since any new and unseen traffic is detected as an attack. Training on normal attack free datasets can help overcome this challenge. Maintaining an updated normal profile in evolving network conditions is a challenge for these techniques.
- Anomaly based detection systems may give high false positive rate when they encounter any legitimate but unusual upward surge in network traffic. For example, flash events are similar to high-rate DDOS attacks and involve a sudden increase in requests per VM, network bandwidth, response time, memory usage, etc. Additional information should be used to explain unusual behaviour that is not an attack.
- The anomaly detection technique must be application agnostic and in multicloud scenario, it should be cloud agnostic as well.
- There is a challenge of being able to identify anomalous patterns across multiple and multivariate network traffic streams.

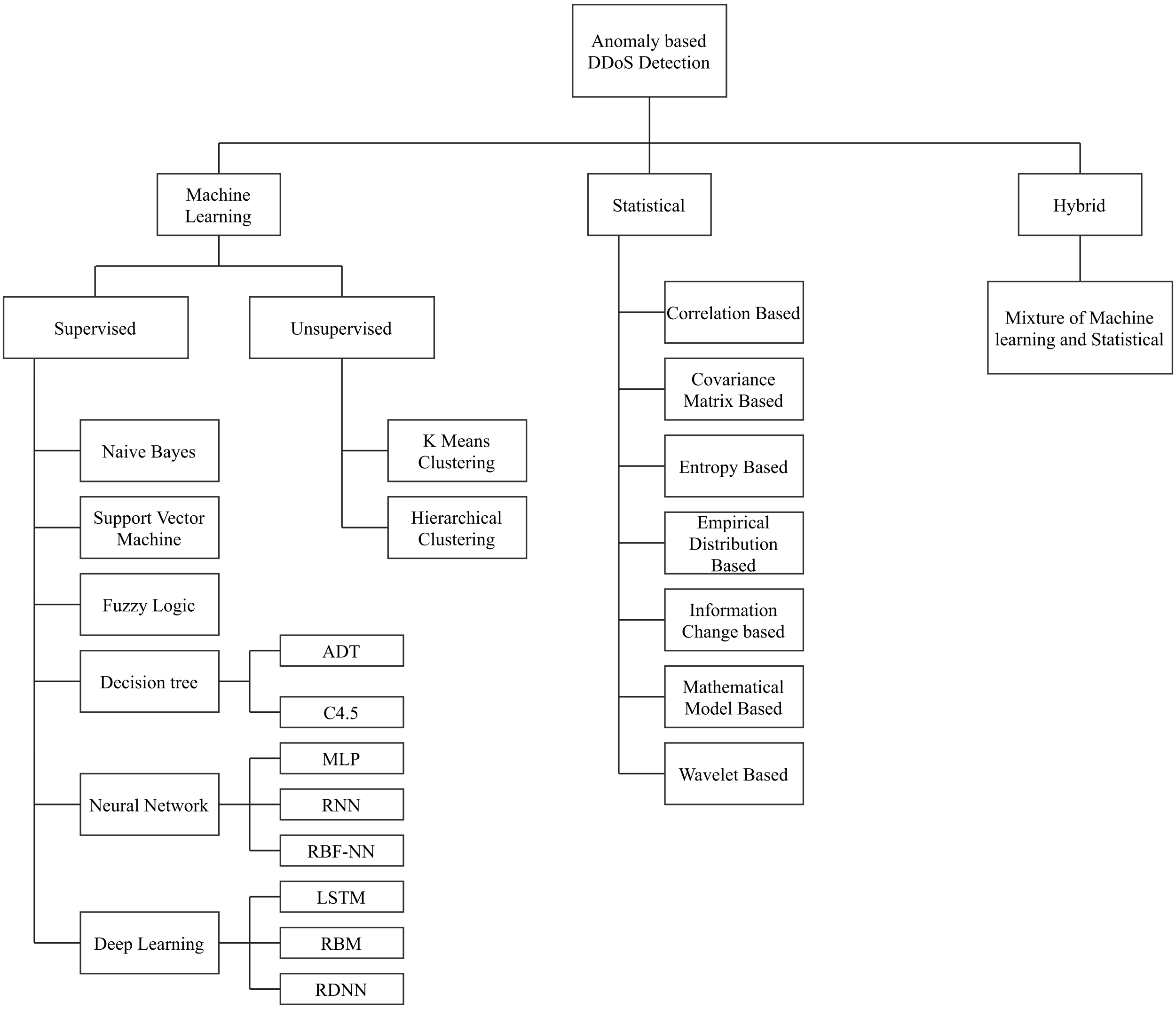

Fig. 4. Anomaly based DDoS detection methods.

- The sheer volume of data in a cloud environment poses a significant scalability challenge to anomaly detection in real time. Trillions of data points from several organizations and users of multitenant cloud need to be handled by the anomaly detection technique.
- The labelled data requirement for training and/or validation of system is generally a substantial problem.
- Traffic may contain noise that behaves in a similar way to the actual anomalies, and hence it becomes tough to differentiate and discard noise.

5.3. Taxonomy of anomaly based DDoS detection methods

Anomaly based DDoS detection methods can be implemented using machine learning, statistical or hybrid techniques. Machine learning based anomaly detection methods automatically learn anomalous behaviour patterns from the attack dataset without the intervention of humans. Machine learning methods are first trained by providing the information about attack features. A model is prepared based on the information gained in training. The model is then used to identify anomalous patterns/attacks in the actual environment. The machine learning methods can be supervised or unsupervised. Supervised method requires labelled training dataset consisting of both normal and anomalous patterns. The unsupervised method does not require labelled training dataset and formulates the rules by analysing the dataset for identifying attack patterns. Examples of machine learning methods include Bayesian Network, Markov Model, Neural Network (NN), Fuzzy Logic, DT, etc.

In statistical methods of anomaly detection, system prepares a statistical model for normal behaviour of the traffic. Data traffic is considered illegitimate if it does not fit into statistical model on the basis of some test statistic. Examples of statistics that can be used are — profiles of hosts, users, workstations, networks, user categories; and statistical measures like frequencies, means, standard deviations, variances, covariances, etc. Statistical tests can be parametric or non-parametric. Parametric techniques have understanding of underlying data distribution and collect parameters from the given data. On the other hand, non-parametric approach does not have understanding of underlying data distribution. The hybrid based anomaly detection method combines the features of both statistical and machine learning methods in a multistep process. Fig. 4 presents a taxonomy of different approaches being used for anomaly based DDoS detection.

5.4. Survey of anomaly detection approaches

In this subsection, different approaches based on anomaly detection for DDoS detection in literature have been investigated w.r.t. various aspects, namely, year of publishing, technique used, viz. machine learning, statistical, or hybrid; dataset, features and tools. The strengths and weaknesses of each method have also been listed.

A survey of network anomaly detection techniques has been presented in [75]. The concept of an anomaly and its detection over a network has been explained. The use of classification methods namely SVM, Bayesian, NN and Rule based approach for anomaly detection is surveyed. Statistical approaches using signal processing, Principal Component Analysis (PCA) and mixture model, information theoretic approaches such as correlation analysis using measures like entropy and information gain, and clustering techniques for detection of anomalies in networks, have been reviewed. Information about available datasets for network intrusion detection has also been provided.

The survey in this paper deals with DDoS detection mechanisms particularly in case of cloud environment and an attempt has been made to include all major recent works up to 2020. The various approaches for anomaly based detection of DDoS attacks are:

5.4.1. Machine learning approaches

Machine Learning approaches have been divided into supervised and unsupervised depending on whether labelled or unlabelled dataset is being used. This section discusses anomaly based supervised and unsupervised machine learning methods in detail. Tables 4 and 5 depict a summary of methods using supervised and unsupervised machine learning for anomaly based DDoS detection with their features, approach, dataset, strengths, and weaknesses.

Supervised Machine Learning Approaches: A supervised NN based approach for anomaly detection has been discussed in [76]. Cloud Trace Back (CTB) solution has been used to identify the origin of attack. It is mainly placed closed to the source of the cloud victim. The request is first sent to the CTB which marks the IP header fields like ID and reserved flag to track the attacker in case of attack. Algebraic method is used for path reconstruction. Cloud Protector is a trained back propagation NN which takes input data values into a weighted network and adds them to check whether they are above predefined threshold or not. It is placed after the CTB to filter out the XML-DoS messages.

An anomaly based system to detect DoS attacks using NB classification has been proposed [77]. The system is primarily designed for transport layer, i.e., TCP and UDP traffic. In the training phase, the system takes the traffic features and the model calculates NB based probabilities for various events and keeps it offline into a data structure. This data structure information works as a deciding information for determining the network as normal or anomalous during the deployment stage.

Chonka and Abawajy [78] have developed ENDER method, i.e., Pre-dEcisioN, advance Decision, lEaRning system. This method detects HX-DOS (HTML and XML) attacks in cloud. ENDER is made up of two algorithms, i.e., CLASSIE and ADMU. First, source address and source tag values are extracted. CLASSIE algorithm is based upon DT which is applied to the extracted values to detect the HX-DOS messages. After this ADMU method, i.e., Added Decision Marking and Update is applied, that works based on likelihood of already classified messages. A small 1-bit mark is associated with the detected HX-DOS messages so that RAD module, i.e., Reconstruct, and Drop, can withdraw these messages prior to reaching the target.

A Web access pattern based method with components for DDoS detection and prevention has been proposed by Masood et al. [79]. In the first stage, image or cryptographic based challenge is given to users for limiting the number of users entering second stage. The users who have correctly solved the challenge will be given a hidden or secret port for further communication so that number of requests at the server is limited. The users are classified as good or bad clients based on resource access patterns. This classification is done with DT algorithm J48. Based on classification results, amount of resources given to good clients are more as compared to bad clients. An anomaly based back propagation neural network based solution is provided against ICMPv6 DDoS flooding attacks in IPv6 network [80]. First the data is preprocessed and filtered to obtain data values containing only Ipv6 packet type. Information gain ratio (IGR) and principal component analysis (PCA) are used to extract the most significant features among the dataset. The packets are aggregated containing number of ICMPv6 packets, source IP address, and destination IP address and these aggregated packets are fed to ANN model using back propagation technique for detection of attacks. Experiments show that the proposed approach has reduced the time to detect attack and achieved detection accuracy 98.3%.

Authors in [81] selected features related to packet and IP. These selected features are given as input to various machine learning algorithms for training and testing. The algorithms used are NB, DT, SVM, Multi Layer Perceptron (MLP) for classification of DDoS attacks. The results showed that DT gives the highest detection accuracy. Information Gain, Gain ratio and Chi-Square methods have been used for feature selection. Balamurugan and Saravanan [82] have developed detection mechanism based on two algorithms, i.e., packet scrutinization algorithm and hybrid algorithm which combines normalized clustering algorithm with recurrent NN (NK-RNN). The packet scrutinization algorithm analyses parameters given in Table 4. Based on this algorithm, port scanning and initial flooding attack is detected. The normalized clustering algorithm removes the non-genuine data by calculating maximum and minimum values of cluster. Then resulting clusters are given to RNN module which trains over this reduced data and determines the malicious packets based on intruder's attributes. One Time Signature (OTS) based algorithm is used for safe data access by users. Signature is generated based on user ID and randomly generated private keys.

An approach called DeepDefense based on deep learning method was proposed [83]. The authors used Deep Recurrent NN (DRNN) for tracing malicious attack activities and learning patterns from attack traffic. RNN is independent of the input window size and can learn from long term sequence of data in shorter time as compared to conventional machine learning methods. The proposed methods reduce the error rate from 7.517% to 2.103% in larger data set.

Authors of [84] have used deep and machine learning approaches for anomaly detection over CIDDS-01 dataset. They have implemented and compared machine learning approaches viz. deep NN with 3 different architectures; stacking with NB, Linear Discrimant Analysis (LDA) and OneR; Variational AutoEncoder (VAE) to synthetically generate minority class samples; Random Forest (RF); and voting on oneR, NB and ExtraTree. Experimental results for two different cases have been reported, one with the original class distribution, and the second with sampling to handle class imbalance. It has been concluded that RF is an effective method where sample size is small, and deep NNs are effective where larger training data is available.

Detection of DDoS attack in IoT networks through network middleboxes has been done using machine learning and flow characteristics of traffic data [85]. IoT specific flow related stateless features, stateful features and handcrafted features have been extracted. These are fed as input to five classifiers, viz., k-nearest neighbour (KNN), DT with Gini impurity, linear SVM, RF using Gini and NN. SVM gave the worst performance, and all other methods gave similar performance. The stateless features were found to be more informative than the stateful ones indicating that this approach is promising and lightweight for detecting IoT specific DoS attacks.

Imamverdiyev [86] proposed DDoS detection method based on Gaussian Bernoulli type multi layer Restricted Boltzmann Machine (RBM). The accuracy of the detection method is improved by optimizing the hyperparameters of the deep RBM model. The proposed method beats the detection results of SVM, radial basis, and DT machine learning methods. Anomaly based approach using NN and Particle Swarm Optimization (PSO) has been used for detection of DDoS attacks in cloud space by Rawashdeh et al. [87].

Sniffer collects the network traffic from virtual cloud environment and stores it as pcap files. The data collected is then preprocessed, i.e., relevant features are extracted and normalized to improve the efficiency of the classifier. The ANN based classifier is trained with PSO for finding optimal weights. The preprocessed data is then fed into the classifier for finding the anomalous behaviour. A new dataset was generated using TCP SYN flood and UDP attack packets for the experimentation. The proposed scheme performs better than ANN based model in respect to accuracy.

Deep learning method based on Long Short Term Memory (LSTM) has been used for detection of DDoS attacks [88]. DDoS defender has been deployed using SDN technology. 192 behavioural features have been extracted from the dataset captured through CTU-13 botnet. SDN blocks the infected packets from propagating to the cloud. The proposed method outperforms other conventional models in terms of accuracy.

In [89], authors have used their own rules which are formulated based upon SNORT. The dataset has been generated using Tor Hammer tool using ownCloud environment. The classifiers: SVM, NB, and RF have been applied on the new data set generated with the help of crafted rules. It has been reported that SVM outperforms all other classifiers in terms of accuracy. Authors [90] used MLP model as a classifier for binary classification of attacks. It uses sequential backward selection method (SBS) which is a wrapper based feature selection method. Authors also devised a feedback mechanism which recreate the model dynamically after considering the detection errors. Authors in [91] presented an efficient Deep Belief network (DBN) and fuzzy classifier for detection of DDoS attacks. Taylor elephant-herd optimization is used for optimizing the weights and biases of the network. Rigorous computer simulations were performed and showed that the proposed method is better than the state-of-the-art methods.

An effective deep learning based anomaly detection method has been proposed against DDoS attacks in [92]. In this method, the preprocessed feature values are applied to Autoencoder (AE) having optimal hyperparameters. The output of the AE contains reduced feature set which is fed to SVM for classification purpose. The author achieved 99.1% accuracy on the virtual traffic generated with Kali Linux. The authors in [93] proposed double PSO based method for selection of relevant feature set and optimal hyperparameters for the classification of attacks. The double PSO consists of an upper level and a lower level. The upper level helps to provide best feature set and lower level provides optimal hyperparameters for deep learning models for effective classification. The effectiveness of three deep learning models, viz. DBN, DNN and Long Short-Term Memory Recurrent Neural Networks (LSTM-RNN) with pre-training using PSO, has been compared. Experimentation on two datasets, viz. CICIDS2017 and NSL-KDD shows improvement in detection rate and reduced FAR.

Unsupervised Machine Learning Approaches: An intrusion detection system consisting of hierarchical clustering and SVM has been proposed [94]. Firstly, the clustering algorithm helps to prepare a reduced high quality dataset. This dataset is the pure representation of all the data points in the former dataset. The produced dataset is given for training and testing to SVM on some selected parameters.

Chen et al. [95] have proposed a detection system to protect key components of cloud computing. This system consists of monitoring agents to collect information from different log files like system, firewall, web; and router access logs for behavioural analysis; and transmission of this information to the cloud. Cloud infrastructure employs Hadoop MapReduce and Spark to increase the speed of data processing. K-means clustering algorithm is used for anomaly detection, wherein the detection results are visualized in web applications for better monitoring of security operations. Authors have proposed a cognitive system having two-step process for detection of DDoS attacks in mobile cloud computing [96]. The two steps are multi-layer traffic screening and decision-based VM selection. The multi-layer traffic screening has two phases: profile-based screen and filter-based screening. In first phase, profile based screening uses client's OS and location information to build a profile of client. The second phase extracts inter delay between packets from incoming traffic. These two phases help in detecting anomalous behaviour by analysing the incoming packets. A combination of K-means clustering and DBSCAN called KD algorithm is used to create optimal number of groups which can enhance the phase 2 filtering process. Then, depending upon the values received, the VM selection procedure shifts the process to another VM to terminate any malicious process. This process prevents the spread of malicious process to other VMs.

5.4.2. Statistical approaches

This section discusses the anomaly based statistical methods provided by various authors in detail. Table 6 depicts a summary of statistical methods for anomaly based DDoS detection with their features, approach, dataset, strengths, and weaknesses.

Authors proposed traditional wavelet analysis and Isomap dimensionality reduction method for DDoS detection [97]. Isomap algorithm reduces the dimensionality of the network traffic and also enhances the significance traffic data. The proposed method enlarges Hurst parameter value for better detection of slow DDoS attacks. Then wavelet analysis method is used to compute self similarity parameter. The comparison with the computed parameter detects normal and abnormal traffic. The proposed method reduced significantly the false positive and false negative in the experimentation.

Idziorek et al. [98] have proposed a detection approach wherein web access logs are analysed and it is verified that genuine web access patterns are in accordance with Zipf distribution and Spearman's footrule distance. The proposed method detects anomalies based on web access patterns training, which are not according to the mentioned pattern.

Dou et al. [99] developed Confidence Based Filtering method (CBF). This method is fast, requires less storage and has good detection accuracy. In non-attack period, the proposed method first fetches the required attribute value pair of IP and TCP header fields from traffic. Correlation value is computed between the extracted fields. Then, the confidence value is calculated for the number of occurrences of the attribute pairs. In attack period, proposed strategy examines CBF score to determine whether the packet is legitimate or not.

Koduru et al. [100] have proposed that Time Spent on Web pages (TSP) can be used to detect anomalous behaviour of attackers. TSP of attacker in case of flooding is negligible or zero. Otherwise it is periodic or constant. Mean Absolute Deviation (MAD) of TSP is considered as an important factor to determine abnormal traffic.

Ismail et al. [101] have proposed a covariance matrix based statistical method used for analysis of the behaviour of network traffic. In the first step, a nominal profile is constructed for non-attack network traffic behaviour. In this profile, the correlation between various IP header fields like RST, FIN, TCP FIN and TCP retries flags is calculated and converted into covariance matrix.

Table 4
Anomaly based supervised machine learning methods for DDoS detection.

Reference	Features	Approach	Dataset	Strength	Weakness
Chonka et al. [76]	NA	Back Propagation NN	Generated dataset from StuPot project	Identify source of attack within short interval	Very large response variance
Vijayasarathy et al. [77]	TCP flags, payload size, source/destination port number and count, source/destination IP address and count, inter-packet time gaps, total connection time till current packet, number of packets in connection	NB based	DARPA and SETS	Lightweight solution that can work in real time	Sensitive to error proportion and abnormal window count parameters
Chonka & Abawajy [78]	Source address and source tag values	DT based	StuPot dataset	Addresses the problem of digital signatures	Attackers are aware of being traced
Masood et al. [79]	Purchasing history, CPU processing time, session information parameters	DT algorithm J48 based	KDD cup 2000	Make available more resources to clients that are in the good list than in bad list	Image based cryptographic challenge consumes significant bandwidth
Saad et al. [80]	Time, source IP, destination IP, length, protocol, flags, destination port, source port	ANN	Real attack traffic from NAv6 laboratory	Provided approach for IPv6 based DDoS attack	Resuts not generalized to other datasets
Meitei et al. [81]	Mean of inter packet arrival time from same IP address, probability of occurrence of an IP per 15 s, resource records, min packet size, max packet size	Classification algorithms DT, MLP, NB, and SVM	CAIDA	Parameter reduction methods improve the performance	Not suitable for encrypted packet headers
Balamurugan & Saravanan [82]	Arrival Time, confidence level, flow distribution and packet count	NK-RNN	NA	OTS method for secured access of data on cloud is provided	RNN is computationally expensive
Yuan et al. [83]	20 features of dataset	DRNN	ISCX2012	Reduces the error rate from 7.517% to 2.103%, can detect different types of attack	Gives high accuracy only if dataset is large
Abdulhammed et al. [84]	Source IP, source Port, destination IP, destination Port, protocol, date, duration, bytes, packets, flags	RF, deep NN, Voting, Stacking	CIDDS-01	High accuracy and DR, low FAR for RF	Results may not generalize to other datasets
Doshi et al. [85]	Packet size, inter packet arrival time, bandwidth, IP address cardinality	KNN, DT with Gini impurity, linear SVM, RF using Gini, NN	Generated using Raspberry Pi v3 devices	Stateful and handcrafted features improved performance of machine learning algorithms	Results need to be validated against standard and/or real world datasets involving more IoT devices
Imamverdiyev & Abdullayeva [86]	38 features of dataset	RBM based	NSL-KDD	Outperforms SVM, radial basis, DT type machine learning methods	Experimentation done on small dataset gave low accuracy
Rawashdeh et al. [87]	13 features like protocol, service, total packet, totalbyte, avg packet size	NN with PSO	Simulated traffic generation	Optimization improves accuracy	Computationally expensive
Priyadarshini & Barik [88]	192 features of attack traffic generated through HPing-3	LSTM	ISCX 2012	Can be used for both fog and cloud environment	Works well for large datasets only
Wani et al. [89]	Duration, protocol, source IP, destination IP, source port, packets, bytes	SVM, NB and RF	Tor Hammer tool for attack traffic generation	Shows superior performance of SVM in classification of attack traffic	Results are not validated against standard dataset
Wang et al. [90]	Wrapper based sequential feature selection	MLP	Generated dataset from ISOT, ISCX and campus network	Effective in selecting optimal features when network is complex and changing	Feedback mechanism generates false positives and false negatives
Velliangiri & Pandey [91]	Source-bytes, destination-bytes, duration, logged_in, count, srv_count, serror_rate, rerror_rate, diff_srv_rate, same_srv_rate, srv_diff_host_rate	DBN and fuzzy	KDD and two simulated datasets	Use of Elephant herd optimzation outperforms state-of-the art methods	Computational cost expensive
Kasim [92]	25 features of dataset	AE and SVM	CICIDS2017 and NSL-KDD	Lower FAR and improved results due to reduced feature set given by AE	Computationally expensive, not suitable for large datasets
Elmasry et al. [93]	10 features of NSL-KDD and 25 features of CICIDS2017	Double PSO with DBN, DNN and LSTM-RNN	CICIDS2017 and NSL-KDD	Detection rate increased by 4% to 6% compared to deep learning models	Computationally expensive

Table 5
Anomaly based unsupervised machine learning methods for DDoS detection.

Reference	Features	Approach	Dataset	Strength	Weakness
Horng et al. [94]	Out of 41 features, 19 features selected for detection of DDoS	Hierarchical Clustering and SVM	KDD cup	Reduced dataset applied to SVM thus decreasing training time	Reconstructing tree in hierarchical clustering can be expensive if threshold keeps changing
Chen et al. [95]	Source IP, destination IP address, source and destination port, packet length, package time stamp	K-means Clustering	Real-world traffic of Chicago Equinix Data Centre	Hadoop and Spark speeds up data processing	Spark introduces processing overhead if the network is small
Dey et al. [96]	Inter packet delay, user profile based on OS and location information	K means and DBSCAN clustering	Simulated data	Reconfigurable according to cloud provider requirements	New approach needs to be applied to varied datasets

The decision of whether the incoming traffic is normal or abnormal is determined by matching the computed covariance matrix of the initial step with covariance of the traffic experienced. An entropy based detection technique has been proposed by Zakarya [102] for DDoS attacks in the cloud space. The entropy rate uses distribution ratio to identify attack flow. Attack packet dropping algorithm is used for detection. Each ingress edge router has anomaly detection system. If it is detected as a DDoS capable attack flow, then this traffic flow is sent to an adjacent router for confirmation. After confirmation that DDoS attack has been detected is received, the packets are discarded.

Vissers et al. [103] have stated that attacks on web service consume resources by forwarding SOAP requests that contain malicious XML content like oversized XML document, oversized encryption, deeply nested XML structures, spoofed Reply To and Fault To addresses. The defence mechanism consists of a filter in the cloud architecture for HTTP header inspection and XML content inspection. First, normal profile is generated using Gaussian Model (GM) for all entries containing SOAP action. To prevent HTTP flooding, the number of requests is limited within a specified time span. The system checks the HTTP header to determine whether the SOAP action is correct or not. If the size of the message exceeds a certain boundary, it is considered as outlier and the corresponding request is rejected. For XML content inspection, first features of XML content are extracted using SAX. SOAP action is checked for spoofing and no illegal WS-addressing requests are made. Each extracted feature is evaluated with corresponding GM. Features are tested for outliers. Finally, the request is forwarded as normal operation.

Alqahtani and Gamble [104] have provided a method to detect DDoS attacks at four different functional levels which are service, tenant, application and cloud. Hash map summarizes the data stream for detection of anomaly at the service level. Alarm is raised for the possible malicious events if the flow rate at the cloud increases heavily. Abstract information distance metric is compared with set threshold to detect the suspicious flow. Flow is categorized as malicious flow, if the calculated value is higher than the pre-defined threshold. The requesters which are responsible for high flow rate are discovered and marked as suspicious. The computed hash map from service level is sent to tenant level, where detectors combine these hash maps to detect possible attackers. At application level, detectors detect the extent of DDoS attacks by correlating DDoS attacks with flow rate for evaluating performance deterioration of web based services. The detection results from above two levels are directed towards the last level, i.e., cloud level for confirmation of attack.

Badve et al. [105] have suggested a statistical based model for DDoS detection system in cloudspace. It uses Generalized Autoregressive Conditional Heteroskedasticity (GARCH) model which is a non-linear time series model that predicts the traffic states by predicting the value of variances and comparing real variance values to detect any potential anomaly in the incoming packets. To further enhance the DR, attack traffic is passed to ANN which categorizes it into attack and normal traffic after removing undesirable points smaller than the predetermined threshold.

Somani et al. [106] have suggested shrink-expand based service resize method which reduces the resources of resource intensive targeted web servers to minimal resources, thereby reducing attack area. Attack condition becomes true if request response time is more than the acceptable request time out at the client side, and if number of established connections are greater than the maximum allowed connections. Then established connections are cleared up by tuning two TCP parameters — TCP fin timeout and TCP retries. This method provides quick resources for mitigation from available resources in presence of attack. A lightweight method for detection of TCP SYN flooding DDoS attack in SDN called SLICOTS has been introduced [107]. It is a rule based system installed on the control plane which blocks the users making a large number of half open TCP connections to prevent flooding by attackers. Experimental results over various scenarios comparing SLICOTS with state-of-the-art method Operetta, have shown that SLICOTS outperforms other method in terms of detection accuracy, time and resources utilized.

An approach for detection of Low rate DDoS (LDoS) attacks based on a hypothesis test which computes t-statistic has been proposed [108]. The presence of LDoS attack has been detected by checking the probability distribution of packet size values for incoming traffic assuming that packet size values are more uniformly distributed in non attack traffic than in attack traffic. DR, FPR and FNR have been computed to evaluate the effectiveness of the proposed approach. An increase in the value of significance level, leads to an increase in the DR and decrease in the FNR. But the FPR increases with increase in significance level. It has been claimed that this approach gives satisfactory performance over DARPA and CAIDA datasets with low computing overhead.

Zareapoor et al. [109] have proposed a two step method for the detection of DDoS attacks. A nominal profile is constructed by extracting header fields. The detection system compares the TTL value with IP to hot count value in order to detect spoofed IP. If there is a mismatch, then the packet is dropped. Then the extracted header fields of incoming packets are compared with nominal profile for attack detection. Jensen–Shannon divergence is used for detecting the deviation between nominal profile and the incoming header fields. Netwag tool was used for generating DDoS attacks. Classifiers like PART, RF, NB and Ripper were compared with proposed system and the results showed that the proposed model has better results in terms of accuracy and processing time.

A scheme which combines feature based and volume based detection to shield against DDoS attacks has been presented [110]. The proposed scheme applies Exponential Moving Average (EMA) to two time series, one having entropy scores and the other having amount of received packets. Hence, this approach integrates

Table 6
Anomaly based statistical methods for DDoS detection.

Reference	Features	Approach	Dataset	Strength	Weakness
Lu et al. [97]	NA	Wavelet analysis using isomap algorithm	KDD and DARPA	Detects weak DDoS attacks	Isomap iterations add an extra computational step
Idziorek et al. [98]	Web activity nature, resource usage, request semantics	Zipf's law, Spearman's Footrule and Overlap based	NASA server webtraces and attack generation through bots	Deals with EDoS	Cannot distinguish attack clients and sudden legitimate requests (Flash Crowd)
Dou et al. [99]	TTL, protocol type, source IP address, TCP flag, destination port number	Confidence based filtering with correlation between features	C++ simulation programme for attack and MAWI working group traffic archive for normal	Less processing speed and requires less storage	Parameters weight adjustment not automatic
Anusha et al. [100]	Time spent on web pages (TSP)	Mean Absolute Deviation (MAD) based	Normal traffic and bot based attack towards eucalyptus cloud	Deals with EDoS	No automation for monitoring of MAD graphs
Ismail et al. [101]	IP header flags — SYN, FIN, RST, TCP retries	Correlation of features in IP header	Hyenae tool for generating attack data	Suitable for large networks	Covariance matrix generation is time consuming
Zakarya [102]	IP address and port no.	Entropy method with attack dropping algorithm	Detection accuracy	Good QoS and no overhead of extra packets	Not suitable for large networks
Vissers et al. [103]	Content length, no. of elements, nesting depth, longest element, attribute, namespace	Parametric technique with Gaussian model	Simulated different attacks	No extra memory and no considerable CPU usage	Protects only cloud broker
Alqahtani and Gamble [104]	Flow rate of requests	Four different functional levels — service, tenant, application and cloud	NA	Suitable for complex cloud environments	Cannot distinguish between Flash crowd and DDoS
Badve et al. [105]	Variance of entropy of group of packets as bins	Generalized Autoregressive Conditional Heteroskedasticity (GARCH) Model based	Simulated data	High DR	Sensitive to size of bins and threshold value
Somani et al. [106]	Number of established connections, request, response time	Service resizing and TCP tuning based technique	Generated real attack instances on cloud	Minimizes overall downtime, provides required resources for mitigation	Overhead of resizing and deciding when to resize
Mohammadi et al. [107]	Source MAC, destination MAC, source TCP port, and destination TCP port	Rule based approach	Simulated different attacks	Does not block legitimate packets	New approach needs to be validated against standard dataset and other methods
Bhushan and Gupta [108]	Source IP and packet size	Hypothesis test based on t-statistic	DARPA and CAIDA	Detects low rate DDoS attacks	Cannot be applied to large networks
Zareapoor and Shamsolmoali [109]	Source IP, TTL, destination IP, ports, IP Flags, length, TCP Flags, ICMP Type and UDP length	Jensen–Shannon divergence	Networking tool for generating attack	Detection module requires less storage	Accuracy is less than RF, Ripper, PART and NB
Bojovic [110]	Diversity of source IP and packet rate	Number of packets and CUSUM algorithm on entropy time series	Academic computer network for generating normal traffic and attack script file for generating attacks	Detects both high rate and low rate attacks	Not able to distinguish denial of service attacks from peer to peer traffic
Conti et al. [111]	Window size, entropy threshold	Periodic monitoring based on traffic analysis statistics	CAIDA	Reduction in bandwidth consumption and request processing, gain in packet delivery rate	New approach needs to be validated against stronger attack scenarios

both volume-based and feature-based detection. The two EMA indicators are applied to two different time series, one having a short period and the other having a long period.

Conti et al. [111] have recently presented some lightweight approaches for DDoS detection in SDN. These approaches are — selective blocking against route spoofing attacks, and periodic monitoring against resource depletion attacks. Flow based detection techniques do not perform well for stealthy and non link based DDoS attacks. Periodic monitoring detects anomalies based on low values of entropy measure and violation of rules related to low traffic flows.

5.4.3. *Hybrid approaches*

This section discusses anomaly based hybrid methods provided by various authors in detail. Table 7 depicts a summary of hybrid methods for anomaly based DDoS detection with their features, approach, dataset, strengths, and weaknesses.

Modi et al. [112] have developed a network intrusion detection system (NIDS) that integrates Snort and Bayesian Classifier in the cloud environment to detect anomalous behaviour in the cloud. It can detect both known and unknown attacks. The experimental results showed that DR is increased and it lowers false positives and false negatives. Bayesian classifier has high accuracy as compared to other classifiers like NN classifier, DT. Unlike [112], radial basis function NN (RBF-NN) has been used for classification of attack traffic in [113]. In this work, 11 features including statistical and flag features are used for training the classifier. Metaheuristic Bat algorithm has been used to optimize the RBF-NN. Firstly, a pre-processing module is used by the researchers [114] which removes the inessential data having low correlation, then it goes to detection module where SNORT detects known attacks by matching pattern with known rules. To check whether the user is legitimate or not, or to detect an unknown attack, a method C4.5 DT is used.

Entropy and classifier based method has been proposed by authors for detection of DDoS attacks [115]. Firstly, entropy of the incoming headers of the network packet is computed using Shannon formula during a specified time window interval. The traffic is then pre-processed to drop the data traffic whose average entropy is out of normal range. This reduced traffic data is input to RF classifier for classifying attacks. A feature construction module which extracts raw features has been defined in [116]. Shannon entropy is used on the raw features to form entropy based regular features. Lyapunov exponent separation calculates rate of separation between different features. Attack detection consist of three classifiers, i.e., RNN, MLP, and Alternating DT (ADT). Traffic is classified as attack and non attack traffic by using simple majority, based on output of these classifiers.

The authors proposed a model in [117] which includes entropy and SVM method for detection of attacks. Firstly the process calculates entropy of tender features like count of source IP address, source port number, destination IP address, destination port number, packet type, and network packets. Then the normalized entropy values are given to SVM for efficient classification of legitimate and non-legitimate users. A hybrid framework was proposed by [118] for DDoS detection. The process in the framework has been divided on the client side and proxy side due to limited resources. At the client side, after data preprocessing best set of features are selected for better training and performance. Then divergence test is applied, if the results are greater than threshold value appropriate action is done to prevent the attack else the data is sent to proxy side. At the proxy side, multiple classifiers NB, RF, DT, MLP, and KNN are used for using the properties and benefits of above algorithms for better performance. KNIME has been used for implementation of the proposed work.

5.5. Observations and summary of anomaly based DDoS methods

Table 8 depicts a summary of methods using machine learning, statistical, and hybrid methods for anomaly-based DDoS detection. These methods are compared using metrics — accuracy, detection time, overhead, adaptability and scalability. The column values Low, Medium and High, depict the respective strength of the metric in the corresponding approach.

The review and analysis of anomaly based methods for DDoS detection indicates that hybrid and machine learning methods give good accuracy as compared to statistical methods. Accuracy of machine learning method heavily depends on quality of training data and statistical methods may not give good accuracy for unseen data. In terms of detection time, machine learning method performs the best since the model is pretrained on training data and detection is fast compared to statistical methods which have to compute the statistical features and metrics on the fly. Hybrid methods that involve a two stage detection scheme are the slowest. In terms of overhead, machine learning and hybrid methods involve more overhead of training the model and multistage detection respectively as compared to statistical. Machine learning and hybrid methods are adaptive as they can learn new attack patterns from the new data. Machine learning methods, particularly deep learning methods, are also more scalable in terms of increasing input traffic and large number of input features. As machine learning gains popularity, additional options like using distributed processing with MapReduce, libraries for hardware acceleration like TensorFlow.js, are becoming available for scalable real time deployment of machine learning based solutions.

As discussed in Section 1, the utility computing model and autoscalability features of cloud computing allow resource scaling and bring in additional economic losses. The multitenancy feature of cloud may lead to collateral damages to non-targets and co-hosted VMs. These factors differentiate between a traditional network DDoS attack and cloud targeted DDoS attack [120].

The methods detailed in Section 5 above have been employed for detection of DDoS attacks targeted at the cloud. The selection of optimal features, preprocessing of dataset, and testing or profiling against the learned rules or patterns, are the common set of tasks performed for detection of DDoS attacks. The CSP monitors the network edge for any anomaly in the traffic behaviour or other performance metrics. The pattern of utilization of cloud resources by VMs is also an important feature in detection of DDoS attack. The hypervisor in virtualized servers can monitor the resource usage of each VM on physical server. An attack can be detected once VMs exceed the set resource utilization thresholds. Detection of anomalies in resource usage of VMs by applying virtual machine introspection has been proposed as a method for the detection of DDoS attacks in [121].

DDoS attackers also use cloud infrastructure for launching attacks by installing botnets. In a cloud DDoS detection scheme, there should be a mechanism to detect the internal attack by VMs in the cloud network. Network level and VM monitor level checks have been proposed to detect presence of any attacker bots running inside hosted VM [122]. Authors have proposed making a list of actions of VMs infected by bots and then applying clustering to identify the malicious VMs based on training [123]. A solution for detection of DDoS attack launched through a cloud of bots has been proposed in [124] wherein the CSP checks the traffic flow and performs the anomaly detection using source traceback techniques. A collaborative DDoS detection technique using Hypervisor based checks to detect the vulnerabilities in the guest VMs has been applied [125]. The dynamic autoscalability feature of the cloud has been used for DDoS mitigation in [126] wherein a DDoS aware resource allocation strategy that segregates traffic and scales up resources based on demands of the legitimate users in the cloud environment, has been proposed.

5.6. Cloud simulation-related framework and datasets

Researchers have used varied platforms for verifying results of methods for detection of DDoS attacks in cloud environment. Survey of literature indicates that experiments have been conducted using cloud simulators and/or using cloud management software on different testbeds. Table 9 depicts following information about different cloud simulation-related framework used for experimentation — name and release year of cloud framework; its developer; and a brief description. Researchers have used one of three approaches for experimentation — simulators, emulators and public/private clouds using Cloud Management Systems (CMS). CMS is a software for operating and managing

Table 7
Anomaly based hybrid methods for DDoS detection.

Reference	Features	Approach	Dataset	Strength	Weakness
Modi et al. [112]	17 out of 41 features of KDD dataset	Snort and Bayesian classifier based	KDD	Compatible with any communication protocol, detects both known and unknown attacks	Computation Overhead
Velliangiri & Premalatha [113]	Source address, destination address, packet type, packet size, packet rate, average packet size, inter arrival time	RBF-NN with Bat algorithm using statistical features	Simulated attack traffic	Speedy learning due to RBF-NN	Computationally complex
Zekri et al. [114]	Protocol, Land, service, TTL, flag	Signature and DT based	Hping3 for attack and python scripts for normal traffic	Scalable and low computational cost	Cannot distinguish between Flash crowd and DDoS
Idhammad et al. [115]	Connection definition features, source/destination IPs, source/destination ports	Information Theoretic Entropy and RF based	CIDDS-001 public dataset	Better accuracy than single classifier methods	FPR fluctuations increase with increase in noisy traffic and detection time is higher than DT
Koay et al. [116]	Separation IP, separation port, separation MAC, separation network, separation TCP	Entropy and multi classifier system	ISCX'12 and DARPA	RNN provides higher precision overall and works well on sequenced data. ANN can model non linear and complex data. ADT can handle missing values well	Computationally complex
Yang [117]	Source IP, source port number, destination IP address, destination port number, packet types, network packets	Information entropy and SVM based	DARPA, KDD and NSL KDD	Suitable for large networks	Limited representation range of entropy leads to detection of attacks in pre-defined range only
Hosseini et al. [118]	Selected subset of features via forward selection corresponding to classifiers	Divergence Test and NB, random forest, decision tree, MLP, KNN based	NSL KDD and dataset generated in [119]	Including multiple classifiers detects vast range of attacks	Overhead of selecting feature subset for each classifier

Table 8
Comparative summary of anomaly based DDoS detection methods.

Approach	Accuracy	Detection time	Overhead	Adaptive	Scalability
Statistical	Medium	Medium	Low	Low	Low
Machine learning	High	High	Medium	High	High
Hybrid	High	Low	Medium	High	High

applications, data and services running through cloud. It ensures that cloud based resources are optimally working and effectively interacting with other users. There are four popular CMSs that have been used for creating public, private and hybrid clouds — Eucalyptus, OpenStack, CloudStack and OpenNebula. The difference between these platforms lies in their architecture, ease of installation, security and administration.

Table 10 shows different datasets that have been used for validating the results in DDoS field. The table provides information about the following aspects — year in which dataset was created; category of dataset, i.e., whether it has been generated in live environment or been captured through simulation; attack type whether HTTP, UDP, TCP, ICMP or DNS; IP address — actual or mapped address; and availability, i.e., whether it is publicly available or not. It has been observed that many papers use KDD, CAIDA and DARPA datasets as they provide the actual representation of the attack scenario and include large number of features which fully describes the attack scenario.

It is noteworthy to mention that different researchers have used different datasets (real or synthetic), or different subsets, or different combinations of same datasets, for experimentation. Hence, it is inappropriate to surmise about performance of DDoS detection methods based on these metrics. This type of a comparison is valid if the same dataset is being used for different experiments. However, there are some papers which cite the same dataset and report common metrics. A comparison of these papers has been presented in Table 11.

It can be seen from Table 11 that machine learning methods are giving promising results in detection of attacks. Machine learning based methods are favourable because they can be applied on new attack data. Various methods like k-means, NB, RF, SVM, DT, ANN, and clustering have been used in literature, but DT and ANN have shown the best results. ANN and DT have given accuracy more than 99% on DARPA, KDD and CAIDA datasets. RF has shown superior performance over CIDDS-01 dataset. There are different datasets containing data for various types of DDoS attacks, but most datasets are not available in complete form due to security concerns. CAIDA is a well-known network layer dataset in the field of DDoS. But after 2016, it has restricted access to few countries only, namely USA, Australia, Canada, Israel, Japan, Netherlands, Singapore and United Kingdom. Also the datasets become outdated and are not true representative of attack scenarios. So, researchers face problems in validating results for DDoS detection in cloud environment as there is no standard or benchmark dataset available. They either have to simulate the attack and capture the data or they impute the data entries. Most of the datasets available are unlabelled so it adds up the burden for first labelling it and then applying machine learning methods.

Table 9
Cloud simulation-related framework.

Framework name	Released year	Developer	Description
Geni [127]	2004	National Science Foundation (NSF)	Virtual lab for networking and distributed systems
Eucalyptus [128]	2008	Eucalyptus Systems Inc.	Open source software creates public, private and hybrid AWS compatible clouds
OpenStack [129]	2010	Rackspace and NASA	Open source software for maintaining public, private and hybrid clouds
GreenCloud [130]	2010	Team at University of Luxembourg	Packet-level simulator for cloud communications with energy saving cloud data centres
Cloud Stack [131]	2011	Developed by cloud.com, acquired by Apache software foundation	Open source software for maintaining public, private and hybrid clouds with abilities simulator to Amazon EC2
Savi [132]	2012	University of Toronto	Multi-tiered SDN enabled cloud testbed
CloudSim (Version 4.0) [133]	2016	Cloud Computing and Distributed Systems Lab	Framework for simulating cloud infrastructures and services
OpenNebula (Version 5.4) [134]	2017	OpenNebula Community	Open Source tool for maintaining public, private and hybrid clouds
Qemu (Version 3.0) [135]	2018	QEMU team: Peter Maydell et al.	Open source software for hardware virtualization
ownCloud (Version 10.2.1) [136]	2019	ownCloud Inc., founded by Markus Rex, Holger Dyroff and Frank Karlitschek	Client server software for file hosting services

Table 10
Datasets used in DDoS area.

Year	Dataset	Dataset category	Traffic type	IP address	Availability
1998	FIFA World cup [137]	Real	HTTP	Mapped	Yes
1999	KDD [138]	Real	TCP	Mapped	Yes
2001	UCLA [139]	Synthetic	UDP	Mapped	Yes
2007	CAIDA [140]	Real	ICMP	Mapped	On request
2009	WITS [141]	Synthetic	UDP	Actual	Yes
2009	DARPA [142]	Synthetic	TCP	Actual	Yes
2012	TUIDS [143]	Synthetic	ICMP, UDP, TCP	Actual	Yes
2012	UNB [144]	Real	HTTP	Actual	On request
2014	Booter [145]	Real	DNS	Actual	Yes
2015	UNSW-NB15 [146]	Synthetic	ICMP, UDP, TCP	Actual	Yes
2017	CIDDS-001 [147]	Synthetic	HTTP	Mapped	Yes

Table 11
Comparison of metrics for different approaches.

Dataset	Reference	Method	Accuracy	FAR
KDD	[94]	Machine learning	95.72%	0.7%
	[112]	Hybrid	91.04%	0.12–1.67
	[117]	Hybrid	100%	0
NSL KDD	[86]	Machine learning	73.23%	0.43%
	[117]	Hybrid	99.97%	0.05%
CAIDA	[81]	Machine learning	96.9–99.3%	97.8-99.3%
	[108]	Statistical	99% TPR	15%–30%
DARPA	[77]	Machine learning	98.7%	1.8%
	[108]	Statistical	99% TPR	15%–30%
	[116]	Statistical	50%–99%	0.2%–40%
	[117]	Hybrid	Unspecified	High
CIDDS-1	[115]	Hybrid	99.54%	0.4%
	[84]	Machine learning	99.99%	le^{-4}%

6. Use case scenarios and laws governing DDoS

In this section, we outline some probable scenarios of DDoS attacks in a cloud environment, their modus operandi and the potential serious consequences in three critical sectors, namely — healthcare, SMBs, and telecommunications. Having highlighted the adverse effects of DDoS in these scenarios, we mention the laws that have been enacted in major nations to act as a deterrent against launching of DDoS attacks.

6.1. Illustrative DDoS attack use case scenarios

This section documents three illustrative use case scenarios which will provide deeper insight into the current DDoS attacks.

- Use Case 1: Disruption of Critical Healthcare Service due to Amplification Attack

Memcached attack is a recent new form of DDoS attack. Memcached is a distributed caching system which temporarily stores content in it and helps to hasten the loading of application and

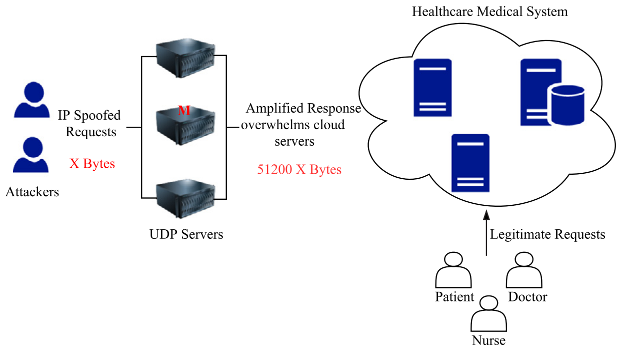

Fig. 5. Disruption of critical healthcare service due to amplification attack.

website content. Memcached has been used by attackers for launching a major DDoS attack wherein the attacker spoofed requests and sends towards memcached servers. There are millions of memcached servers distributed around the globe and are exposed without any authentication. These servers receive the data and amplify it before sending to the target server. The amplification factor is massive which is up to 51200x. These unsecured servers can be used to flood a large amount of traffic against critical infrastructures like healthcare systems, powerhouses, financial organizations, etc. leading to tremendous losses.

Fig. 5 shows how an attacker can initiate a memcached DDoS attack leading to delays and disruption of the healthcare system. Healthcare sector is particularly susceptible to cloud based DDoS attacks since ailments are being increasingly treated with cloud based monitoring services and various IoT devices like infusion pumps, pacemakers, MRI machines, etc. are storing and relaying information over the cloud. The illustrative EpicCare server provides services for clinical care, decision support and streamlined processes. In this scenario, the attacker spoofs a request and sends it to a memcached server, which is a UDP server. The server receives the request, amplifies it and sends it to the server hosting the patient healthcare records and information. Since the amplification is large, eventually, the server slows down and service gets disrupted, and the server may become unresponsive shutting down the healthcare system for legitimate healthcare providers. Moreover, the attack can be a ransomware having soft target, in this case, health and lives of patients. The health care system stores complete Electronic Medical Records (EMR) of patients, case history, previous test reports, next appointments, specific case information, etc. The outage on healthcare system can lead to serious consequences for patients and doctors alike.

- Use Case 2: Economic Denial of Service due to Multivector Attack

Multivector DDoS attack is a relatively new and complex form of DDoS attack that is gaining notoriety these days. This attack has lead to significant impact in recent incidents. Instead of involving a simple attack technique, it combines different techniques, which makes it harder to detect. For example, it can have a blend of different types of amplification attacks. Botnets like Mirai combine ten different kind of DDoS attack vectors which can morph over time. This makes detection a difficult task. The mitigation for such attacks has to be multi-layered. Fig. 6 shows a sample multi vector DDoS attack. In this figure, command and control server infects vulnerable IoT devices — smart phones, home security appliances, DVRs etc. and makes botnets. These bots then launch multi vector DDoS attack. The attack is a blend of volumetric attack, protocol exploitation attack and application layer attack. The attack is targeted towards cloud which has 4 servers, S1, S2, S3 and S4. The attacker attacks S2 server for disrupting it services. When the S2 server dies, the processes running on it may be migrated to new server S3 depending on the VM migration policy, or alternatively, there can be autoscalability in which new resources can be added up to the existing server. In either case, due to the billing and elastic provisioning policies in cloud computing, DDoS then leads to EDoS attack as customers get charged for extra resource consumption.

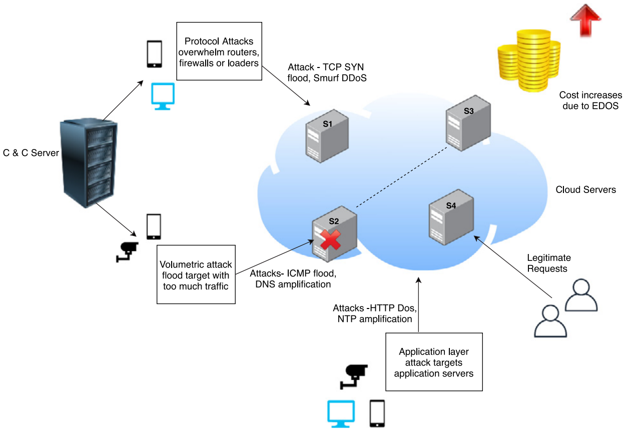
Protocol Attacks overwhelm routers, firewalls or loaders
Attack - TCP SYN flood, Smurf DDoS
Cost increases due to EDOS
C & C Server
S1
S3
Cloud Servers
S2
S4
Volumetric attack flood target with too much traffic
Attacks- ICMP flood, DNS amplification
Legitimate Requests
Attacks -HTTP Dos, NTP amplification
Application layer attack targets application servers

Fig. 6. Economic denial of service due to multivector attack.

- Use Case 3: Business Loss to Communication Service Provider (CSP) due to Stealthy Attacks

Low rate Denial of Service (LDoS) is a big threat to cloud computing as it is stealthy in nature and appears similar to normal traffic. The data is sent towards the target after a short interval of time for exploiting the TCP congestion control mechanism. The process is repeated over intervals leading to denial of service. A related type of attack mechanism used these days is a bit and piece attack, wherein attacker sends attack traffic on several different IP addresses to evade the detection system. The detection system cannot decide which of these several addresses it should act on. Fig. 7 depicts a scenario in which LDoS is combined with bit and piece attack on infrastructure of a Communication Service Provider (CSP). Disrupting CSP services will affect business organizations and consumers that use CSP for communication. Geographically dispersed attackers send bursts of packets after a short interval of time. These packets target different IP addresses instead of a single IP address. Hence, this forms a stealthy attack which successfully dodges the detection system and disrupts the CSP services causing business and reputation losses to CSP as well as its customers.

6.2. Laws governing DDoS attacks

DDoS attacks are illegal and a criminal offence. In major countries the attacker is subjected to criminal and civil liability which may include fine or imprisonment. It is considered unlawful by reputed organizations like National Crime Agency, Federal Bureau of Investigation (FBI) etc. Most countries have incorporated serious statutory measures to deal with incidents of DDoS attacks and protect national security. Table 12 shows laws and regulations for DDoS of some leading countries. The Tallinn Manual 2.0 is an analysis by the International Group of Experts (IGE) of how international law applies to cyber operations. According to Tallinn Manual 2.0, any interference with an object enjoying sovereign immunity is considered as a violation of international law. DDoS attack is also constituted under violation of sovereign immunity.

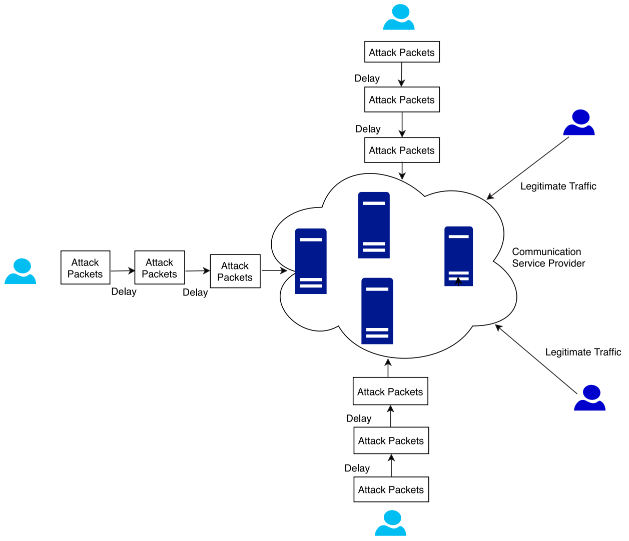

Fig. 7. Business Loss to Communication Service Provider (CSP) due to stealthy attacks.

DoS attacks are considered a federal crime in the United States of America, under the Computer Fraud and Abuse Act (CFAA), with penalties that include years of imprisonment. The Computer Crime and Intellectual Property Section of the US Department of Justice deals with cases of DoS/DDoS. This act applies to any person or computer who affects electronic communications regardless of whether the person is located within US boundaries. The people that take part in DDoS attacks run the risk of being charged with legal offences at the federal level, both criminally and civilly, according to the law (Title 18 U.S.C., section 1030). The criminal is prosecuted and may get up to 10 years imprisonment.

Budapest convention is the first multilateral treaty addressing the issue of computer related crimes. The Council of Europe along with Philippines, Canada, Japan, South Africa and the United States of America drafed this convention. The convention promises that these countries will change their local laws to get in line with rules and regulations written in this cybercrime convention. Sixty three states have ratified and four states have signed the convention up to March 2019.

The Cybercrime Convention Committee of Europe criminalizes DDoS attacks under T-CY Guidance Note 5. DDoS attacks are covered by the conventions listed in Articles 2, 4, 5, 11 and 13. These articles are issued according to what an attack actually does. Article 2 - Illegal access (computer system may be accessed), Article 4 - Data interference (delete, damage, deteriorate, suppress or alter data), Article 5 — System interference (hamper the functioning of the computer system), Article 11 — Attempt, aiding and abetting (DDoS attack may aid several other crimes like forgery, computer related fraud, violation of copyright etc.) and Article 13 — Sanctions (the criminals are punishable under this article according to the type of DDoS crime).

In France, the Article No. 88–19 of 5 January 1988 on software fraud covers the criminality of hacking and DDOS attacks. This act was amended in 2004 and 2013 and, more recently, by the Act no. 2015–912 of 24 July 2015. Subsequent amendments in 2004, 2013 and by the Act no. 2015–912 in July 2015 doubled some fines and increased all applicable penalties.

In Germany, Hacking/DDOS attacks are often considered as criminal offence according to Section 202a of the German Criminal Code (Strafgesetzbuch — StGB) (data espionage), section 303a StGB (alteration of data), and/or section 303b StGB (computer sabotage). Particularly, section 303b applies to DDoS attacks. The provision states that a person who causes considerable data processing interference by rending unusable, removing or altering a data processing device, thereby causing financial loss, criminal activity or compromising critical infrastructures, is liable for imprisonment penalties of up to 10 years.

The UK legal system under the Computer Misuse Act (CMA) 1990, makes it illegal to hamper the operation of a computer system or impair access to programmes/data unless the person is authorized. DDoS attacks are thus treated as a criminal offence under Section 3 of the CMA-unauthorized acts with intent to impair the operation of a computer. Distributing DDoS launch tools is also treated as an offence. In England and Wales, the maximum penalty is 12 months in prison and 6 months in Scotland but may go up to 10 years if the case goes to full trial in a Crown Court before a jury. The statutory maximum fine by magistrate's court is £5,000. The Police and Justice Act 2006, which amended Section 3 of the Computer Misuse Act 1990, particularly outlaws denial-of-service attacks and sets a maximum penalty of 10 years in prison.

Under Article 286 of the Criminal Law of the People's Republic of China, DDoS attack is considered as the crime of disrupting computer information systems and imprisonment of more than 5 years may be given in serious cases. In Australia, DDoS attack is recognized as a type of high tech crime offence defined in Commonwealth legislation within Part 10.7 — Computer Offences, as codified in the Criminal Code Act 1995. It is criminalized under section 477.3 of the Code. DDoS attack comes under the jurisdiction of Australian police when the affected computer, system, or server is in Australia, or there is an Australian citizen among the persons involved. The maximum penalty for carrying out DDoS attack is 10 years imprisonment. Electronic Communications and Transactions Act (ECT) of South Africa considers DDoS attacker guilty under article 86 Section 5. The criminal is punished with imprisonment for a term of up to 5 years or can be charged with a heavy fine. In Brazil, under the Criminal Code (Law No. 2848/1940), the act of attacking a computing device, whether connected to the internet or not, by breach of a security mechanism and for the purpose of collecting, altering or destroying data or information or installing vulnerabilities to obtain an illegal benefit is deemed as crime.

According to the Information Technology Act 2000 in India, if a person causes denial of access to the owner of the systems, it qualifies as hacking and is punishable with imprisonment for a term up to 3 years and/or fine up to INR 500,000. DDoS attacks may be also be charged under "theft" and "criminal trespass" under Indian Penal Code, 1860 and are punishable with imprisonment and/or fine. DDoS attacks are illegal in Canada under section 342 of the Criminal Code with a liability of imprisonment not exceeding 10 years. DDoS attacks are also covered by Section 430(1.1) – Mischief of computer data – to obstruct, interrupt or interfere with the lawful use of computer data, to obstruct, interrupt or interfere with a person in the lawful use of computer data or to deny access to computer data to a person who is entitled it.

As the global data protection landscape continues to evolve, it is expected that more nations will adopt stringent laws and penalties to deter attackers from launching DDoS attacks in future.

7. Future research directions

In this section, we discuss some of the open research issues in DDoS detection in a cloud environment and recommend possible future research directions.

Table 12
Laws governing DDoS.

Country	Law	Year	Article/Section	Penalty
Australia [148]	Criminal Code Act	1995	Commonwealth legislation within Part 10.7 – Computer Offences	Imprisonment of up to 10 years
Brazil [149]	Brazilian Criminal Code	1940	266	Imprisonment of 3 years and may be doubled in the case of public calamity
Canada [150]	Criminal Code	1985	342	Fine and imprisonment up to 10 years or punishable on summary conviction
China [151]	Criminal Law	1997	286	Imprisonment of more than 5 years given in serious cases
France [152]	French Criminal Code	1994	323–2	Imprisonment of 5 years and fine up to £150,000; imprisonment of 7 years and fine up to £300,000 when government or public system involved
India [153]	Information Technology Act	2000	66F	Imprisonment up to life
South Africa [154]	Electronic Communications and Transactions Act (ECT)	2002	86–5	Fine (not specified) or imprisonment up to 5 years
UK [148]	Computer Misuse Act	1990	3	England and Wales — Imprisonment up to 12 months; Scotland — imprisonment from 6 months up to 10 years if the case goes to full trial; Statutory maximum fine by magistrates court is £5000
USA [155]	CFAA	1984	1030	Imprisonment up to 10 years

7.1. Research area: Attacks using IoT devices

IoT devices are prone to attacks since they are always connected, often poorly configured, and lack basic security protocols. Due to constrained resources, IoT devices cannot run memory or computation intensive machine learning algorithms. Authors of [18] have provided a survey of DDoS defence solutions in IoT. There are few methods surveyed that are tailored specifically for IoT devices and these are based on machine learning.

Issues:

- Current research on attacks on cloud using IoT is still in nascent stage with works focussing on handling a particular type of attack only. A machine learning based DDoS detection method for IoT has been proposed in [85]. Feature selection using IoT-specific network behaviour has been proposed, before applying machine learning based classifier. It is proposed that network middleboxes can be used to detect DDoS attack sources based on flow characteristics of network traffic in a lightweight and protocol independent manner. Further research is needed to check the validity on traffic from various IoT devices and real DDoS attack patterns.
- There is no standard or benchmark dataset available to validate the performance of proposed methods for detection of DDoS launched using IoT devices.
- Cloud DDoS detection methods need to be implemented and tested against different attack vectors in IoT environment. However, there is no standard test bed or platform for IoT security.

Future Research Directions:

- Examination of the evolving DDoS attacks that are currently being launched by exploiting the vulnerabilities in unsecured IoT devices.
- Checking of the external validity of DDoS detection methods for IoT devices by collecting and standardizing large datasets.
- Employing deep learning methods for detection of DDoS related to IoT [85].
- Investigation of whether some types of IoT device are more responsive to anomaly based detection [85].

7.2. Research area: DDoS and software defined networking

SDN offers decoupling of control and data plane, centralized control and traffic based network analysis, which makes the cloud more dynamic, manageable and scalable. But SDN can itself become target of DDoS attacks on — application layer by attacking northbound API or application; control layer by attacking controller, northbound/southbound/eastbound/westbound API; or infrastructure layer by attacking switch or southbound API. Authors of [156] have proposed CENSOR, a new secure and scalable cloud-enabled IoT architecture over SDN paradigm, that includes an IoT controller and an IoT agent component. An attacker can launch DDoS on SDN controller and bring the entire network down. To deal with this issue, CENSOR proposes an efficient hierarchical (two level) software remote attestation to secure the network, reduce bandwidth consumption and latency. Fog computing IoT controllers at edge SDN switches pre-process data for a secure and scalable IoT architecture by acting as IoT gateways, which apply security checks. Since SDN itself is a new architecture, more work is needed to develop this architecture and test its efficacy for DDoS defence in integrated IoT SDN environment.

Issues:

- Software Defined Networking requires lightweight solutions to detect and mitigate the effect of DDoS attacks [111].
- SDN does not provide visibility into application layer. So detecting application layer attacks using deep packet inspection results in degradation of data plane [157].
- The tradeoff between availability and security of cloud resources that arises out of auto-scaling, needs to be addressed.

Future Research Directions:

- Development and validation of lightweight DDoS detection solutions.
- Development of detection methods for application layer DDoS that can address performance versus security tradeoff.
- Comparison of various deep learning models to detect DDoS attacks in conjunction with SDN in the fog network or at the edge of the cloud is another research direction [88].
- Detection and mitigation of DDoS attacks in a network with multiple SDN controllers [158].

- Development of intelligent and adaptive user centric cloud pricing and resource provision models.

7.3. Detection of multivector and new DDoS attacks

Multivector attacks are a combination or chain of different attacks such as multiple network-layer attacks or multiple application-layer attacks. These attacks are perpetrated with the intention of circumventing current DDoS defence mechanisms by changing the attack vector during the course of ongoing attack. An example is a blend of UDP flood with NTP amplification. Multivector attacks are harder to detect than single attacks because a single type of attack quickly begins and ends. Even when it gets detected, by the time the DDoS mitigation measures are initiated, the vector is changed to next chained one, resulting in a large number of resources being used for defence. Additionally, there are other new sophisticated attack vectors such as stealthy attacks, carpet bombing attacks, that are continually surfacing in the cloud environment.

Issues:

- The increasing sophistication of DDoS on cloud services, and cloud components like VMs, using new attack vectors.
- No study has been carried out on detection of multivector attacks.

Future Research Directions:

- Detection of application layer DDoS attacks since current defence solutions are not widely adopted [16].
- Investigation of attacks that can damage co-hosted VMs such as Memory DoS attacks that can lead to severe performance degradation and denial for co-hosted VMs [159].
- Development of a multithreaded approach for detection and mitigation of multivector DDoS attacks.

7.4. Multilayer defence

As discussed previously, DDoS attacks in cloud are becoming increasingly sophisticated, often involving multiple layer attacks and targeting multiple points of the cloud environment. In order to defend against such attacks, the defence solutions also have to be multilayer by including on-demand cloud data scrubbing for volumetric attacks, as well as on-premise and inline packet inspection based detection mechanisms for other attacks. The defence solutions have to be a combination of on-premise perimeter based as well as in-cloud based defence.

Issues:

- Modern organizations are moving towards multicloud environments and virtualized data centres, due to which, there is no single point of control and monitoring available to protect against DDoS.

Future Research Directions:

- A broader level of protection and defence mechanism is required to detect and handle threats. Multilayer defence involving application level defence using VM isolation in multitenant clouds; system level defence using VM/OS, hypervisor security; and external level defence using filtering at edge routers by ISPs [11]; is the need of the hour.

8. Conclusion

Despite the numerous scientific and commercial solutions that have been developed for detection of DDoS attacks, the frequency and severity of these attacks has increased in modern day multicloud computing environments. These attacks often have devastating consequences, particularly for the users and providers of cloud-based services. The defining characteristics of cloud environment, namely, autoscaling, multitenancy and pay-as-you-go can worsen the impact of such attacks. Furthermore, as organizations move towards multiple cloud environments, the DDoS attack detection systems need to be adapted further. There is a substantial need to relook into the existing solutions to mitigate the ill effects of DDoS. Anomaly based techniques for detection of DDoS attacks hold the potential to solve this problem as they can be improved to be intelligent enough to handle unseen or unknown attacks as well as known attacks and their derivatives. This paper presents a taxonomy of DDoS attacks; list of emerging DDoS attacks in cloud environment and their impact; use cases, laws, commercial solutions, survey of anomaly detection techniques for DDoS detection; challenges faced while deploying such techniques and their advantages. Detailed survey and analysis of recent attacks and detection techniques indicates that employing machine learning methods for anomaly based detection of DDoS attacks in the cloud, is the most promising direction. This survey can guide in designing and implementing an effective and intelligent solution to detect DDoS attacks, particularly in the current day multitenant cloud space.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This research work is supported by Technical Education Quality Improvement Project III (TEQIP III) of MHRD, Government of India assisted by World Bank under Grant Number P154523 and sanctioned to UIET, Panjab University, Chandigarh (India).

References

[1] E. Brown, NIST Issues Cloud Computing Guidelines for Managing Security and Privacy, National Institute of Standards and Technology Special Publication 800-144, 2012.

[2] Peter Mell, Tim Grance, Effectively and securely using the cloud computing paradigm, NIST Inf. Technol. Lab. 2 (8) (2009) 304–311.

[3] Reuven Cohen, Cloud attack: Economic denial of sustainability (EDoS), 2019, (Accessed May 4, 2019). URL http://www.elasticvapor.com/2009/01/cloud-attack-economic-denial-of.html.

[4] Casey Crane, The 15 top DDoS statistics you should know in 2020, 2019, (accessed Nov 14, 2019). URL https://cybersecurityventures.com/the-15-top-ddos-statistics-you-should-know-in-2020.

[5] Verisign. Verisign Releases Q1 2017 DDOS Trends Report. URL http://www.digitalterminal.in/news/verisign-releases-q1-2017-ddos-trends-report/9642.html.

[6] Paul Nicholson, 5 most famous ddos attacks. URL https://www.a10networks.com/blog/5-most-famous-ddos-attacks/.

[7] Tomer Shani, Updated: This ddos attack unleashed the most packets per second ever. here's why that's important, 2019, (Accessed September 3, 2019). URL https://www.imperva.com/blog/.

[8] Jay Thakkar, DDoS attack statistics: A look at the most recent and largest DDoS attacks, 2019, (Accessed Oct 19, 2020). URL https://sectigostore.com/blog/ddos-attack-statistics-a-look-at-the-most-recent-and-largest-ddos-attacks/.

[9] Kaspersky, Summertime and the DDoS is easy: Q2 saw 18% rise in attacks compared to last year, 2019, (Accessed July 4, 2019). URL https://www.kaspersky.com/about/press-releases/.

[10] Opeyemi Osanaiye, Kim-Kwang Raymond Choo, Mqhele Dlodlo, Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework, J. Netw. Comput. Appl. 67 (2016) 147–165.

[11] Gaurav Somani, Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti, Rajkumar Buyya, DDoS attacks in cloud computing: Issues, taxonomy, and future directions, Comput. Commun. 107 (2017) 30–48.

[12] Adrien Bonguet, Martine Bellaiche, A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing, Future Internet 9 (3) (2017) 43.

[13] B.B. Gupta, Omkar P. Badve, Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment, Neural Comput. Appl. 28 (12) (2017) 3655–3682.

[14] Neha Agrawal, Shashikala Tapaswi, Defense schemes for variants of distributed denial-of-service (DDoS) attacks in cloud computing: A survey, Inf. Secur. J.: Glob. Perspect. 26 (2) (2017) 61–73.

[15] Sabah Alzahrani, Liang Hong, et al., A survey of cloud computing detection techniques against ddos attacks, J. Inf. Secur. 9 (01) (2017) 45.

[16] Amit Praseed, P. Santhi Thilagam, Ddos attacks at the application layer: Challenges and research perspectives for safeguarding web applications, IEEE Commun. Surv. Tutor. 21 (1) (2019) 661–685.

[17] Jin B. Hong, Armstrong Nhlabatsi, Dong Seong Kim, Alaa Hussein, Noora Fetais, Khaled M. Khan, Systematic identification of threats in the cloud: A survey, Comput. Netw. 150 (2019) 46–69.

[18] Mikail Mohammed Salim, Shailendra Rathore, Jong Hyuk Park, Distributed denial of service attacks and its defenses in IoT: a survey, J. Supercomput. (2019) 1–44.

[19] Shi Dong, Khushnood Abbas, Raj Jain, A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments, IEEE Access 7 (2019) 80813–80828.

[20] Jagdeep Singh, Sunny Behal, Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions, Comp. Sci. Rev. 37 (2020) 100279.

[21] Link11, Link11 ddos report for Europe, 2019, (Accessed May 15, 2019). URL https://www.link11.com/en/ddos-report/.

[22] Thomas Pohle, Biggest DDoS attacks of 2018, 2019, (Accessed May 15, 2019). URL https://www.link11.com/en/blog/biggest-ddos-attacks-of-2018/.

[23] Mohit Kumar, Biggest-ever ddos attack (1.35 tbs) hits github website, 2018, (Accessed July 25, 2019). URL https://thehackernews.com/2018/03/biggest-ddos-attack-github.html.

[24] Scott Hilton, Dyn analysis summary of friday october 21 attack, 2016, (Accessed Oct 25, 2019). URL https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack.

[25] Gloria Omale, Gartner identifies top 10 strategic IoT technologies and trends, 2018, (Accessed September 25, 2018). URL https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends.

[26] Ekaterina Badovskaya Oleg Kupreev, Alexander Gutnikov, DDoS attacks in Q4 2018, 2009, (Accessed May 4, 2019). URL https://securelist.com/ddos-attacks-in-q4-2018/89565/.

[27] Doug Olenick, European bank targeted in massive packet-based ddos attack, 2020, (Accessed June 30, 2020). URL https://www.bankinfosecurity.com/european-bank-targeted-in-massive-packet-based-ddos-attack-a-14505.

[28] Catalin Cimpanu, AWS said it mitigated a 2.3 tbps DDoS attack, the largest ever, 2020, (Accessed June 30, 2020). URL https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever.

[29] Mike Moore, Wikipedia goes offline following DDoS attack, 2019, (Accessed Jan 12, 2020). URL https://www.techradar.com/in/news/wikipedia-taken-down-after-major-ddos-attack.

[30] Jonathon Sheiber, Telegram faces DDoS attack in China…again, 2019, (Accessed Jan 12, 2020). URL https://techcrunch.com/2019/06/12/telegram-faces-ddos-attack-in-china-again.

[31] Lila Kee, Shedding more light on the first U.S. electric grid attack, 2019, (Accessed Oct 6, 2019). URL https://securityboulevard.com/2019/09/shedding-more-light-on-the-first-u-s-electric-grid-attack.

[32] Catalin Cimpanu, Cambodia's ISPs hit by some of the biggest ddos attacks in the country's history, 2018, (Accessed Oct 3, 2019). URL https://www.zdnet.com/article/cambodias-isps-hit-by-some-of-the-biggest-ddos-attacks-in-the-countrys-history.

[33] Jasmine Henry, Ubisoft games, final fantasy 14 affected by ddos attacks, 2018, (Accessed Oct 6, 2019). URL https://gamerant.com/ubisoft-games-final-fantasy-14-ddos-attacks.

[34] Janene Pieters, Dutch banks ABN AMRO, ING hit in cyber attack, 2018, (Accessed Oct 6, 2019). URL https://nltimes.nl/2018/01/29/dutch-banks-abn-amro-ing-hit-cyber-attack.

[35] Pierluigi Paganini, Massive DDoS attack hit the danish state rail operator DSB, 2018, (Accessed Oct 6, 2019). URL https://securityaffairs.co/wordpress/72530/hacking/rail-operator-dsb-ddos.html.

[36] Mark Mayne, 'First true' native IPv6 DDoS attack spotted in wild, 2018, (Accessed Oct 6, 2019). URL https://www.scmagazineuk.com/first-true-native-ipv6-ddos-attack-spotted-wild/article/1473177.

[37] Scott Ferguson, Arbor networks: 1.7tbit/s DDoS attack sets record, 2018, (Accessed Oct 7, 2019). URL https://www.darkreading.com/abtv/ddos/arbor-networks-17tbit-s-ddos-attack-sets-record/a/d-id/741202.

[38] Mike Lenon, Business wire hit by ongoing DDoS attack, 2018, (Accessed Oct 7, 2019). URL https://www.securityweek.com/business-wire-hit-ongoing-ddos-attack.

[39] Chaitanya Kulkarni, Dutch banking giants hit by DDoS attack, 2018, (Accessed Oct 7, 2019). URL http://www.theindiancapitalist.com/2018/01/dutch-banking-giants-hit-by-ddos-attack.html.

[40] Naveen Goud, Latvia E-health system comes under cyber attack from abroad!, 2018, (Accessed Oct 7, 2019). URL https://www.cybersecurity-insiders.com/latvia-e-health-system-comes-under-cyber-attack-from-abroad.

[41] Anthony Coggine, Bitfinex undergoing DDoS attack, IOTA wallets temporarily unavailable, 2018, (Accessed Oct 7, 2019). URL https://cointelegraph.com/news/bitfinex-undergoing-ddos-attack-iota-wallets-temporarily-unavailable.

[42] Iain Thomson, Dreamhost smashed in DDoS attack: Who's to blame? Take a guess..., 2017, (Accessed Oct 23, 2019). URL https://www.theregister.co.uk/2017/08/24/dreamhost_massive_ddos.

[43] Shubham Verma, Google removes nearly 300 apps from play store that hijacked android devices for DDoS attacks, 2017, (Accessed Oct 23, 2019). URL https://gadgets.ndtv.com/apps/news/google-play-store-300-apps-wirex-ddos-attack-akamai-1743535.

[44] Leon Spencer, DDoS attack takes out melbourne IT DNS servers, 2017, (Accessed Oct 23, 2019). URL https://www.arnnet.com.au/article/617665/ddos-attack-takes-melbourne-it-dns-servers.

[45] Dima Bekerman, Avishay Zawoznik, 650 Gbps DDoS attack from the leet botnet, 2017, (Accessed Oct 23, 2019). URL https://www.imperva.com/blog/650gbps-ddos-attack-leet-botnet.

[46] Thomas Johnson, Hackers attack lonestar MTN network, 2016, (Accessed Oct 23, 2019). URL https://www.liberianobserver.com/news/hackers-attack-lonestar-mtn-network.

[47] Pierluigi Paganini, 150,000 IoT devices behind the 1Tbps DDoS attack on OVH, 2016, (Accessed Oct 25, 2019). URL https://securityaffairs.co/wordpress/51726/cyber-crime/ovh-hit-botnet-iot.html.

[48] Krebs on security, Krebsonsecurity hit with record DDoS, 2016, (Accessed Oct 25, 2019). URL https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos.

[49] Zack Whittaker, Biggest ever web attack on BBC actually wasn't even close, 2016, (Accessed Oct 25, 2019). URL https://www.zdnet.com/article/tango-down-bbc-was-this-the-largest-ddos-web-attack.

[50] Kim Zetter, Inside the cunning, unprecedented hack of Ukraine's power grid, 2016, (Accessed Oct 25, 2019). URL https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid.

[51] Richard Chirgwin, Linode: Back at last after ten days of hell, 2016, (Accessed Oct 24, 2019). URL https://www.theregister.co.uk/2016/01/04/linode_back_at_last_after_ten_days_of_hell.

[52] Marek Majkowski, 400 Gbps: Winter of whopping weekend DDoS attacks, 2016, (Accessed Oct 24, 2019). URL https://blog.cloudflare.com/a-winter-of-400gbps-weekend-ddos-attacks.

[53] Jeremy Seth Davis, Sony PSN downed; hacking group claims DDOS attack, 2016, (Accessed Oct 24, 2019). URL https://www.scmagazine.com/sony-psn-downed-hacking-group-claims-ddos-attack/article/527821/.

[54] Alan Martin, Rackspace knocked offline by huge DDoS attack, 2014, (Accessed Oct 24, 2019). URL https://www.welivesecurity.com/2014/12/24/rackspace-knocked-offline-huge-ddos-attack/.

[55] Stephanie Mlot, DDoS attack puts code spaces out of business, 2014, (accessed May 14, 2018). URL https://in.pcmag.com/internet/52898/news/ddos-attack-puts-code-spaces-out-of-business.

[56] Eastern Daylight Time, The world market for ddos protection 2019-2024: Projected to grow at a CAGR of 24.9% with BFSI expected to hold a significant share - researchandmarkets.com, 2019, (Accessed July 28, 2019). URL https://www.businesswire.com/news/home/20190524005248/en/World-Market-DDoS-Protection-2019-2024-Projected-Grow.

[57] Daniel Smith, 2019 predictions: Will cyber serenity soon be a thing of the past?, 2018, (Accessed August 14, 2019). URL https://blog.radware.com/security/2018/11/2019-predictions-will-cyber-serenity-soon-be-a-thing-of-the-past/.

[58] Saman Taghavi Zargar, James Joshi, David Tipper, A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks, IEEE Commun. Surv. Tutor. 15 (4) (2013) 2046–2069.

[59] Akamai, Kona site defender, 2019, (Accessed May 16, 2019). URL https://www.akamai.com/us/en/products/security/kona-site-defender.jsp.

[60] AWS, AWS shield, 2019, (Accessed May 16, 2019). URL https://aws.amazon.com/shield/.

[61] Netscout, DDoS attack protection products, 2019, (Accessed May 4, 2019). URL https://www.netscout.com/products/arbor-ddos-attack-protection/.

[62] AT&T, Distributed denial of service (DDoS) defense, 2019, (Accessed May 16, 2019). URL https://www.business.att.com/products/ddos-protection.html.

[63] CDN77, DoS DDoS mitigation, 2019, (Accessed May 14, 2019). URL https://www.cdn77.com/ddos-mitigation.

[64] Check Point Software Technologies, DDoS protector, 2019, (accessed August 14 2019). URL https://www.checkpoint.com/downloads/products/ddos-protector-appliance-datasheet.pdf.

[65] Cloudflare, Cloudflare spectrum - DDoS protection for TCP and UDP, 2019, (Accessed May 16, 2019). URL https://www.cloudflare.com/lp/cloudflare-spectrum/.

[66] Corero, DDoS attack protection and mitigation, 2019, (Accessed May 14, 2019). URL https://www.corero.com/.

[67] Fortinet, DDoS protection-fortiddos, 2019, (accessed May 14, 2019). URL https://www.fortinet.com/products/ddos/fortiddos.html.

[68] Imperva, Imperva incapsula DDoS protection, 2018, (Accessed May 15, 2019). URL https://www.imperva.com/resources/datasheets/ddos-protection.pdf.

[69] Kaspersky, Kaspersky DDoS protection, 2019, (Accessed May 16, 2019). URL https://www.kaspersky.com/.

[70] Microsoft Azure, DDoS protection, 2019, (Accessed May 15, 2019). URL https://azure.microsoft.com/en-in/services/ddos-protection/.

[71] Sucuri, DDoS protection and mitigation, 2019, (Accessed May 15, 2019). URL https://sucuri.net/ddos-protection/.

[72] Verizon, DDoS shield, 2019, (Accessed May 14, 2019). URL https://enterprise.verizon.com/products/security/secure-gateway-services/ddos-shield/.

[73] Omar E. Elejla, Mohammed Anbar, Bahari Belaton, ICMPv6-based DoS and DDoS attacks and defense mechanisms, IETE Tech. Rev. 34 (4) (2017) 390–407.

[74] Varun Chandola, Arindam Banerjee, Vipin Kumar, Anomaly detection: A survey, ACM Comput. Surv. (CSUR) 41 (3) (2009) 15.

[75] Mohiuddin Ahmed, Abdun Naser Mahmood, Jiankun Hu, A survey of network anomaly detection techniques, J. Netw. Comput. Appl. 60 (2016) 19–31.

[76] Ashley Chonka, Yang Xiang, Wanlei Zhou, Alessio Bonti, Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks, J. Netw. Comput. Appl. 34 (4) (2011) 1097–1107.

[77] Rajagopalan Vijayasarathy, Serugudi Venkataraman Raghavan, Balaraman Ravindran, A system approach to network modeling for DDoS detection using a naive Bayesian classifier, in: Proceedings of 3rd International Conference on Communication Systems and Networks (COMSNETS 2011), IEEE, 2011, pp. 1–10.

[78] Ashley Chonka, Jemal Abawajy, Detecting and mitigating HX-DoS attacks against cloud web services, in: Proceedings of 15th International Conference on Network-Based Information Systems (NBiS), IEEE, 2012, pp. 429–434.

[79] Muddassar Masood, Zahid Anwar, Syed Ali Raza, Muhammad Ali Hur, Edos armor: a cost effective economic denial of sustainability attack mitigation framework for e-commerce applications in cloud environments, in: Proceedings of 16th International Multi Topic Conference (INMIC), IEEE, 2013, pp. 37–42.

[80] Redhwan M.A. Saad, Mohammed Anbar, Selvakumar Manickam, Esraa Alomari, An intelligent icmpv6 ddos flooding-attack detection framework (v6iids) using back-propagation neural network, IETE Tech. Rev. 33 (3) (2016) 244–255.

[81] Irom Lalit Meitei, Khundrakpam Johnson Singh, Tanmay De, Detection of DDoS DNS amplification attack using classification algorithm, in: Proceedings of International Conference on Informatics and Analytics, ACM, 2016, p. 81.

[82] V. Balamurugan, R. Saravanan, Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation, Cluster Comput. (2017) 1–13.

[83] Xiaoyong Yuan, Chuanhuang Li, Xiaolin Li, Deepdefense: identifying ddos attack via deep learning, in: Proceedings of IEEE International Conference on Smart Computing (SMARTCOMP), IEEE, 2017, pp. 1–8.

[84] Razan Abdulhammed, Miad Faezipour, Abdelshakour Abuzneid, Arafat AbuMallouh, Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic, IEEE Sensors Lett. 3 (1) (2018) 1–4.

[85] Rohan Doshi, Noah Apthorpe, Nick Feamster, Machine learning DDoS detection for consumer internet of things devices, in: Proceedings of IEEE Security and Privacy Workshops (SPW), IEEE, 2018, pp. 29–35.

[86] Yadigar Imamverdiyev, Fargana Abdullayeva, Deep learning method for denial of service attack detection based on restricted boltzmann machine, Big Data 6 (2) (2018) 159–169.

[87] Adnan Rawashdeh, Mouhammd Alkasassbeh, Muna Al-Hawawreh, An anomaly-based approach for ddos attack detection in cloud environment, Int. J. Comput. Appl. Technol. 57 (4) (2018) 312–324.

[88] Rojalina Priyadarshini, Rabindra Kumar Barik, A deep learning based intelligent framework to mitigate ddos attack in fog environment, J. King Saud Univ.-Comput. Inf. Sci. (2019).

[89] Abdul Raoof Wani, Q.P. Rana, U. Saxena, Nitin Pandey, Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques, in: Proceedings of Amity International Conference on Artificial Intelligence (AICAI), IEEE, 2019, pp. 870–875.

[90] Meng Wang, Yiqin Lu, Jiancheng Qin, A dynamic MLP-based DDoS attack detection method using feature selection and feedback, Comput. Secur. 88 (2020) 101645.

[91] S. Velliangiri, Hari Mohan Pandey, Fuzzy-taylor-elephant herd optimization inspired deep belief network for DDoS attack detection and comparison with state-of-the-arts algorithms, Future Gener. Comput. Syst. (2020).

[92] Ömer Kasim, An efficient and robust deep learning based network anomaly detection against distributed denial of service attacks, Comput. Netw. 180 (2020) 107390.

[93] Wisam Elmasry, Akhan Akbulut, Abdul Halim Zaim, Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic, Comput. Netw. 168 (2020) 107042.

[94] Shi-Jinn Horng, Ming-Yang Su, Yuan-Hsin Chen, Tzong-Wann Kao, Rong-Jian Chen, Jui-Lin Lai, Citra Dwi Perkasa, A novel intrusion detection system based on hierarchical clustering and support vector machines, Expert Syst. Appl. 38 (1) (2011) 306–313.

[95] Zhijiang Chen, Guobin Xu, Vivek Mahalingam, Linqiang Ge, James Nguyen, Wei Yu, Chao Lu, A cloud computing based network monitoring and threat detection system for critical infrastructures, Big Data Res. 3 (2016) 10–23.

[96] Saurabh Dey, Qiang Ye, Srinivas Sampalli, A machine learning based intrusion detection scheme for data fusion in mobile clouds involving heterogeneous client networks, Inf. Fusion 49 (2019) 205–215.

[97] Liang Fu Lu, Mao Lin Huang, Mehmet A Orgun, Jia Wan Zhang, An improved wavelet analysis method for detecting DDoS attacks, in: 2010 Fourth International Conference on Network and System Security, IEEE, 2010, pp. 318–322.

[98] Joseph Idziorek, Mark Tannian, Doug Jacobson, Detecting fraudulent use of cloud resources, in: Proceedings of 3rd ACM Workshop on Cloud Computing Security, ACM, 2011, pp. 61–72.

[99] Wanchun Dou, Qi Chen, Jinjun Chen, A confidence-based filtering method for DDoS attack defense in cloud environment, Future Gener. Comput. Syst. 29 (7) (2013) 1838–1850.

[100] Anusha Koduru, TulasiRam Neelakantam, S. Mary Saira Bhanu, Detection of economic denial of sustainability using time spent on a web page in cloud, in: Proceedings of IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), IEEE, 2013, pp. 1–4.

[101] Mohd Nazri Ismail, Abdulaziz Aborujilah, Shahrulniza Musa, AAmir Shahzad, Detecting flooding based DoS attack in cloud computing environment using covariance matrix approach, in: Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, ACM, 2013, p. 36.

[102] Muhammad Zakarya, DDoS verification and attack packet dropping algorithm in cloud computing, World Appl. Sci. J. 23 (11) (2013) 1418–1424.

[103] Thomas Vissers, Thamarai Selvi Somasundaram, Luc Pieters, Kannan Govindarajan, Peter Hellinckx, DDoS defense system for web services in a cloud environment, Future Gener. Comput. Syst. 37 (2014) 37–45.

[104] Sarra Alqahtani, Rose F. Gamble, DDoS attacks in service clouds, in: Proceedings of 48th Hawaii International Conference on System Sciences (HICSS), IEEE, 2015, pp. 5331–5340.

[105] Omkar P. Badve, B.B. Gupta, Shingo Yamaguchi, Zhaolong Gou, DDoS detection and filtering technique in cloud environment using GARCH model, in: Proceedings of IEEE 4th Global Conference on Consumer Electronics (GCCE), IEEE, 2015, pp. 584–586.

[106] Gaurav Somani, Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti, Rajkumar Buyya, Service resizing for quick DDoS mitigation in cloud computing environment, Ann. Telecommun. 72 (5–6) (2017) 237–252.

[107] Reza Mohammadi, Reza Javidan, Mauro Conti, Slicots: An SDN-based lightweight countermeasure for TCP SYN flooding attacks, IEEE Trans. Netw. Serv. Manag. 14 (2) (2017) 487–497.

[108] Kriti Bhushan, B.B. Gupta, Hypothesis test for low-rate DDoS attack detection in cloud computing environment, Procedia Comput. Sci. 132 (2018) 947–955.

[109] Masoumeh Zareapoor, Pourya Shamsolmoali, M. Afshar Alam, Advance DDOS detection and mitigation technique for securing cloud, Int. J. Comput. Sci. Eng. 16 (3) (2018) 303–310.

[110] P.D. Bojović, I. Bašičević, Stanislav Ocovaj, M. Popović, A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method, Comput. Electr. Eng. 73 (2019) 84–96.

[111] Mauro Conti, Chhagan Lal, Reza Mohammadi, Umashankar Rawat, Lightweight solutions to counter ddos attacks in software defined networking, Wirel. Netw. 25 (5) (2019) 2751–2768.

[112] Chirag N. Modi, Dhiren R. Patel, Avi Patel, Rajarajan Muttukrishnan, Bayesian classifier and snort based network intrusion detection system in cloud computing, in: Proceedings of 3rd International Conference on Computing Communication & Networking Technologies (ICCCNT), IEEE, 2012, pp. 1–7.

[113] S. Velliangiri, J. Premalatha, Intrusion detection of distributed denial of service attack in cloud, Cluster Comput. (2017) 1–9.

[114] Marwane Zekri, Said El Kafhali, Noureddine Aboutabit, Youssef Saadi, DDoS attack detection using machine learning techniques in cloud computing environments, in: Proceedings of 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), IEEE, 2017, pp. 1–7.

[115] Mohamed Idhammad, Karim Afdel, Mustapha Belouch, Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest, Secur. Commun. Netw. 2018 (2018).

[116] Abigail Koay, Aaron Chen, Ian Welch, Winston K.G. Seah, A new multi classifier system using entropy-based features in DDoS attack detection, in: Proceedings of International Conference on Information Networking (ICOIN), IEEE, 2018, pp. 162–167.

[117] Chen Yang, Anomaly network traffic detection algorithm based on information entropy measurement under the cloud computing environment, Cluster Comput. (2018) 1–9.

[118] Soodeh Hosseini, Mehrdad Azizi, The hybrid technique for DDoS detection with supervised learning algorithms, Comput. Netw. 158 (2019) 35–45.

[119] Mouhammd Alkasassbeh, Ghazi Al-Naymat, Ahmad Hassanat, Mohammad Almseidin, Detecting distributed denial of service attacks using data mining techniques, Int. J. Adv. Comput. Sci. Appl. 7 (1) (2016) 436–445.

[120] Gaurav Somani, Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti, DDoS attacks in cloud computing: collateral damage to non-targets, Comput. Netw. 109 (2016) 157–171.

[121] Min Du, Feifei Li, ATOM: Automated tracking, orchestration and monitoring of resource usage in infrastructure as a service systems, in: 2015 IEEE International Conference on Big Data (Big Data), IEEE, 2015, pp. 271–278.

[122] Joseph Latanicki, Philippe Massonet, Syed Naqvi, Benny Rochwerger, Massimo Villari, Scalable cloud defenses for detection, analysis and mitigation of ddos attacks, in: Future Internet Assembly, Citeseer, 2010, pp. 127–137.

[123] Mohammad Reza Memarian, Mauro Conti, Ville Leppänen, Eyecloud: A botcloud detection system, in: 2015 IEEE Trustcom/BigDataSE/ISPA, Vol. 1, IEEE, 2015, pp. 1067–1072.

[124] Baohui Li, Wenjia Niu, Kefu Xu, Chuang Zhang, Peng Zhang, You can't hide: a novel methodology to defend DDoS attack based on botcloud, in: International Conference on Applications and Techniques in Information Security, Springer, 2015, pp. 203–214.

[125] Hammi Badis, Guillaume Doyen, Rida Khatoun, A collaborative approach for a source based detection of botclouds, in: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), IEEE, 2015, pp. 906–909.

[126] Gaurav Somani, Abhinav Johri, Mohit Taneja, Utkarsh Pyne, Manoj Singh Gaur, Dheeraj Sanghi, DARAC: DDoS mitigation using DDoS aware resource allocation in cloud, in: International Conference on Information Systems Security, Springer, 2015, pp. 263–282.

[127] Raytheon BBN Technologies, Geni, 2019, (accessed August 14 2019). URL https://www.geni.net/about-geni/what-is-geni/.

[128] Wolski, Eucalyptus: An open source infrastructure for cloud computing, 2018, (Accessed August 12, 2019). URL https://www.usenix.org/conference/lisa-09/eucalyptus-opensource-infrastructure-cloud-computing.

[129] Rocky, OpenStack, 2018, (Accessed August 30, 2019). URL https://www.openstack.org/.

[130] Universite Du Luxembourg, GreenCloud, 2010, (Accessed August 30, 2019). URL https://greencloud.gforge.uni.lu/.

[131] The Apache Software Foundation, Apache cloudstack, 2017, (Accessed August 12, 2019). URL https://cloudstack.apache.org/.

[132] University of Toronto, Smart applications on virtual infrastructure (SAVI), 2019, (accessed August 14 2019). URL https://www.savinetwork.ca/.

[133] Mithesh Soni, The cloudsim framework: Modelling and simulating the cloud environment, 2014, (Accessed August 12, 2019). URL https://opensourceforu.com/2014/03/cloudsim-framework-modelling-simulating-cloud-environment/.

[134] Miren Karamta, An introduction to opennebula, 2017, (Accessed August 12, 2019). URL https://opensourceforu.com/2017/02/an-introduction-to-opennebula/.

[135] QEMU, QEMU, 2018, (Accessed August 12, 2019). URL https://www.qemu.org.

[136] ownCloud, OwnCloud, 2019, (Accessed August 28, 2019). URL https://owncloud.com/.

[137] Worldcup, WorldCup98, 1998, (Accessed August 27, 2019). URL http://ita.ee.lbl.gov/html/contrib/worldcup.html.

[138] UCI KDD, KDD cup 1999 data, 1999, (Accessed August 12, 2019). URL http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[139] UCLA Computer Science Department, Trace format, 2001, (Accessed August 12, 2019). URL http://www.lasr.cs.ucla.edu/ddos/traces/.

[140] Center for Applied Internet Data Analysis, The CAIDA DDoS attack 2007 dataset, 2016, (Accessed August 16, 2019). URL https://www.caida.org/data/passive/ddos-20070804_dataset.xml.

[141] Emile Aben, The waikato internet traffic storage (WITS) passive datasets, 2010, (Accessed August 16, 2019). URL https://labs.ripe.net/datarepository/data-sets/the-waikato-internet-traffic-storage-wits-passive-datasets.

[142] Lincoln Laboratory, 1999 DARPA intrusion detection evaluation data set, 1999, (Accessed August 16, 2019). URL https://www.ll.mit.edu/r-d/datasets/1999-darpa-intrusion-detection-evaluation-data-set.

[143] Tezpur University, TUIDS, 2012, (Accessed August 16, 2019). URL http://agnigarh.tezu.ernet.in/~dkb/resources.html.

[144] UNB, ISCXIDS2012, 2012, (Accessed August 16, 2019). URL https://www.caida.org/data/passive/ddos-20070804_dataset.xml.

[145] Simplewiki, Booters, 2014, (Accessed August 16, 2019). URL https://www.simpleweb.org/wiki/index.php/Traces.

[146] Nour Moustafa, Jill Slay, The UNSW-NB15 data set description, 2016, (Accessed August 16, 2019). URL https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/.

[147] Sarah Wunderlich Markus Ring, Dominik Grudl, CIDDS-001 dataset, 2017, (Accessed August 16, 2019). URL https://www.hs-coburg.de/fileadmin/hscoburg/WISENT_cidds_Technical_Report.pdf.

[148] Infosec, Legality of DDoS: Criminal deed vs. Act of civil disobedience, 2019, (Accessed August 10, 2019). URL https://resources.infosecinstitute.com/legality-ddos-criminal-deed-vs-act-civil-disobedience/#gref.

[149] Daniel Pitanga Bastos De Souza, Brazil: Cybersecurity 2019, 2019, (accessed Ausust 10, 2019). URL https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/brazil.

[150] Government of Canada, Justice law website, 2019, (Accessed August 10, 2019). URL https://laws-lois.justice.gc.ca/eng/acts/c-46/.

[151] Government of China, Criminal law of the people's republic of China, 2019, (Accessed August 10, 2019). URL https://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm.

[152] Fredric Lecomte and Victoire Redreaumetadier, France: Cybersecurity 2019, 2019, (Accessed August 10, 2019). URL https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/france.

[153] Government of India, Information technology act 2000, 2016, (Accessed August 10, 2019). URL https://meity.gov.in/content/information-technology-act-2000.

[154] South African Government, Electronic communications and transactions act, 2019, (Accessed August 10, 2019). URL https://www.gov.za/documents/electronic-communications-and-transactions-act.

[155] US Government, 8.2. laws that may apply to DDoS attacks, 2019, (Accessed August 10, 2019). URL http://users.atw.hu/denialofservice/ch08lev1sec2.html.

[156] Mauro Conti, Pallavi Kaliyar, Chhagan Lal, CENSOR: Cloud-enabled secure IoT architecture over SDN paradigm, Concurr. Comput.: Pract. Exper. 31 (8) (2019) e4978.

[157] Qiao Yan, F. Richard Yu, Qingxiang Gong, Jianqiang Li, Software-defined networking (SDN) and distributed denial of service (ddos) attacks in cloud computing environments: A survey, some research issues, and challenges, IEEE Commun. Surv. Tutor. 18 (1) (2015) 602–622.

[158] Mauro Conti, Ankit Gangwal, Manoj Singh Gaur, A comprehensive and effective mechanism for ddos detection in SDN, in: Proceedings of 13th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2017, pp. 1–8.

[159] Tianwei Zhang, Yinqian Zhang, Ruby B. Lee, Memory dos attacks in multi-tenant clouds: Severity and mitigation, 2016, arXiv preprint arXiv:1603.03404.

Aanshi Bhardwaj received her Masters of Engineering in Information Technology from UIET, Panjab University, India in 2014. She is currently a Ph.D. Research Scholar at UIET, Panjab University, India. Her research interests include web mining, machine learning, and security in cloud computing. She has an experience of 5 years in teaching.

Veenu Mangat received her Masters of Engineering in Computer Science and Engineering from Punjab Engineering College (PEC) in 2004 and Ph.D. in Engineering and Technology (Computer Science) in 2016 from Panjab University, India. She is currently working as Associate Professor in Information Technology at UIET, Panjab University. She has a teaching experience of more than 15 years. Her areas of research include data mining, machine learning, privacy and security. She is co-Principal Investigator in research project on 'Monitoring of Active Fire Locations and Precision in Allied Agricultural Activities using Communication Technologies' funded by Ministry of Electronics & IT of Government of India worth Rs. 75.75 lakhs from 2020 to 2022. She has also worked on research project entitled 'Pedestrian Detection from Thermal Imaging' funded by Design Innovation Centre of Ministry of HRD and consultancy project in the area of machine learning. She has edited 2 international volumes and authored 1 book in the area of data mining and machine learning. She has successfully guided 21 Masters of Engineering dissertations and is currently guiding 7 Ph.D. scholars.

Renu Vig received her Ph.D. degree in Engineering and Technology in the field of Artificial Intelligence and Neural Networks from Punjab Engineering College in 1997. She is ex-Director, UIET and currently working as Professor of Electronics and Communications Engineering at UIET, Panjab University, India. She has guided more than 12 PhDs and successfully completed several research projects funded by the Government of India and corporate sector. She has published more than 120 research papers in reputed journals and conferences. Her research interests include fuzzy systems, artificial intelligence, neural networks and next generation networking technologies.

Subir Halder received his M. Tech. and Ph.D. degrees in computer science and engineering from Kalyani Government Engineering College and Indian Institute of Engineering Science and Technology, India in 2006 and 2015, respectively. He is currently a Postdoctoral Researcher at University of Padua, Italy. Prior to that, he was Assistant Professor in the Department of Computer Science and Engineering, Dr. B. C. Roy Engineering College, India. His research interests include security and privacy in next generation networking including WSN, IoT, connected car, network modelling and analysis, and performance evaluation and optimization. He has co-authored more than 35 papers in reputed international peer-reviewed conferences and journals in his field.

Mauro Conti is Full Professor at the University of Padua, Italy, and Affiliate Professor at the University of Washington, Seattle, USA. He obtained his Ph.D.from Sapienza University of Rome, Italy, in 2009. After his Ph.D., he was a Postdoc Researcher at Vrije Universiteit Amsterdam, The Netherlands In 2011 he joined as Assistant Professor the University of Padua, where he became Associate Professor in 2015, and Full Professor in 2018. He has been Visiting Researcher at GMU (2008, 2016), UCLA (2010), UCI (2012, 2013, 2014, 2017), TU Darmstadt (2013), UF (2015), and FIU (2015, 2016, 2018). He has been awarded with a Marie Curie Fellowship (2012) by the European Commission, and with a Fellowship by the German DAAD (2013). His research is also funded by companies, including Cisco, Intel, and Huawei. His main research interest is in the area of security and privacy. In this area, he published more than 250 papers in topmost international peer-reviewed journals and conference. He is Area Editor-in-Chief for IEEE Communications Surveys & Tutorials, and Associate Editor for several journals, including IEEE Communications Surveys& Tutorials, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, and IEEE Transactions on Network and Service Management. He was Programme Chair for TRUST 2015, ICISS 2016, WiSec 2017, and General Chair for SecureComm 2012 and ACM SACMAT 2013.