A Detailed Analysis on Intrusion Identification Mechanism in Cloud Computing and Datasets

Aws Naser Jaber[1(✉)], Shahid Anwar[2], Nik Zulkarnaen Bin Khidzir[3], and Mohammed Anbar[1,2,3]

[1] Faculty of Creative Technology and Heritage, Universiti Malaysia Kelantan, 16300 Bachok, Kelantan, Malaysia
naserjaber.a@gmail.com
[2] Department of Software Engineering, The University of Lahore, Lahore, Pakistan
[3] Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Gelugor, Penang, Malaysia

Abstract. Today, rather than utilizing high-powered workstation/ desktop to access Internet services, users can use small portable devices for this purpose. As such, the computing power is provided via the innovative cloud computing technology, in which computations are performed in remote huge data centers. Applications are conveyed as services on the web in the field of cloud computing. Despite most organizations show significant interest in cloud computing, many clients are not willing to move their vital information to the clouds due to security concern (hacking). Data storage security is one of the greatest challenges in implementing cloud computing. If this issue is not addressed properly, it would hinder the growth of cloud computing. This research study provides a detailed analysis on intrusion identification mechanism in the cloud computing and datasets on the bases of our in-depth understanding.

Keywords: Intrusion identification · Cloud computing · Cyber security

1 Introduction

A cloud is a special IT domain created for providing measured and scalable IT resources remotely [2]. The word was initially used to describe the Internet, which refers to a system of networks that remotely provides access to various distributed IT resources. Before an IT industry sector was formally established for cloud computing, the Internet was commonly represented with a cloud symbol in several widespread documentation and specifications of cyberspace architectures [4].

An effective way of minimizing the required resources of an organization or institution and improving their potentials is through distributed computing. This implies that distributed computing helps institutes to broaden their IT

M. Anbar et al. (Eds.): ACeS 2020, CCIS 1347, pp. 550–573, 2021.
https://doi.org/10.1007/978-981-33-6835-4_37

capabilities. It is important to stress that distributed computing has become a fundamental aspect of the IT industry. Distributed computing is regarded as a new and effective method for business expansion. There is a growing concern for the protection of sensitive data against internal and external attacks on the Internet, as more people and organizations continue to store their applications and data on the cloud.

Cloud computing offers on-demand web access to properly arranged computing resources, and it is considered as a suitable model [7]. There are seven layers in cloud computing, which include User, Application, Middleware, Operating system, Network, Hardware, and Facility. These seven layers are shown in Fig. 1, where the hardware layer consists of network equipment and computer hardware, and the cloud facility is the solid structure that contains the network and the physical hardware, which is also called data centre [8].

Although cloud-based computing keeps attracting a lot of interest, many clients are scared of uploading their personal data on the clouds because of security concern. As long as hackers are keen on getting organizations' data, security is a serious concern. If such concerns are not addressed, they will keep disrupting the growth of distributed computing.

An overview of previous research works on cloud computing, DDoS and H-IDPS is provided in this paper. A general background of cloud computing, as well as its security challenges, is presented in Sect. 2.2. DDoS is critically reviewed in Sect. 2.3 to show how DDoS attack influences the cybersecurity world, especially in cloud computing. Hypervisor, a critical component of virtual server, is discussed in Sect. 2.4. In a bid to highlight the existing security issues, Sect. 2.5 provides a review of DDoS attacks in cloud-based computing. Sections 2.6 and 2.7 respectively contain discussions on IDS and IDPS. A summary of recent works pertaining to IDPS and DDoS attack is given in Sect. 2.8. However, it appears that these layers are implemented in various combinations by cloud service providers, which leads to the formation of three major classes of cloud services [9]. IaaS (Infrastructure as a Service) is the first category of cloud service, and it deals with providing infrastructure software and hardware [10]. A typical example of this type of cloud service is EC2 or Elastic Cloud Computing Service [11]. The second category of cloud service, which is known as PaaS (Platform as a Service), involves the provision of resources for testing and applying user application. A classic example is the Google App Engine [12]. SaaS (Software as a Service) is the third category of cloud service [13], and it is the most commercialized cloud service. Examples of the SaaS-category of cloud service are the Salesforce and Live Mesh of Microsoft [14].

An important component of cloud computing that portrays its value is virtualization [15]. It deals with the process of running a desired program in a virtual environment developed on a server in existence, without affecting other services that the host platform or server provides to other users [16]. The virtual environment can exist as a single instance or as a mixture of different storage devices, computing environments, application or network servers, and operating systems [17]. As shown in Fig. 2, it is easy to understand the concept of virtualization after looking at the various types of virtualization [18]. Risk reduction,

better accessibility, optimal use of resources, and cost reduction are some of the benefits of virtualization [19].

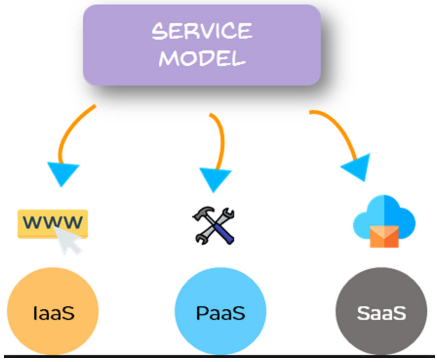

Fig. 1. Layers of a standard cloud-based computing technique

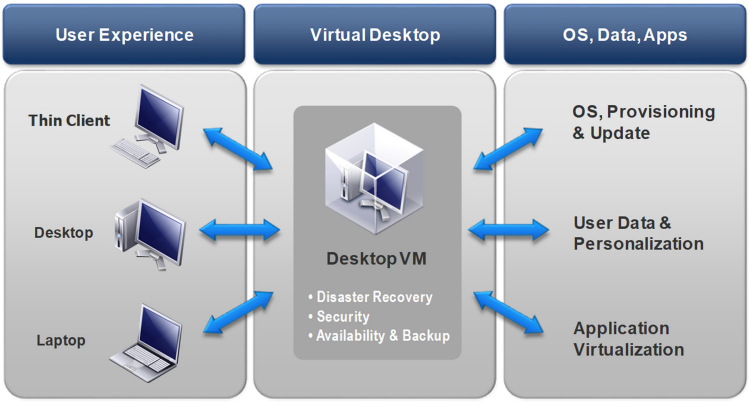

Fig. 2. VM architecture and virtual architecture

The computer hardware, firmware, or software that produces and operates virtual machines is called a hypervisor [20]. A host machine is the computer which a hypervisor uses in running at least one virtual machine, and a guest machine refers to each virtual machine [21]. The hypervisor creates a virtual operating platform for the guest operating systems as well as controls its execution [22]. Virtualized hardware resources may be shared among several instances of operating systems.

When moving services from a physical to a virtual realm, organizations would inarguably increase their threat envelope [20]. In a physical realm, most threats are found in external network and internal network. In the virtual realm, the

attack surface has effectively increased. Sheinidashtegol and Galloway paid a high attention to the additional threat vectors from within the hypervisor itself, and there are several other security considerations that need to be made to counter the risks of those related threats [25]. There are various proposed solutions for the choices of hypervisor. For instance, the Xen hypervisor and other hypervisor systems often use Eucalyptus.

Kaspersky Lab and B2B International conducted an IT Security Risks Survey in which the company representatives that used virtualization technology were interviewed [29]. 15% of enterprises used different versions of commercial platforms based on KVM, and another 16% planned to implement them in the next two years [29]. Free versions were used by 8% of large organizations, with 16% of them planned to introduce them later.

2 Comprehensive Review

One of the greatest challenges in implementing cloud computing is data storage security. The burden of local storage and maintenance is eliminated by the cloud environment, as it allows users to store their data remotely [30]. Nevertheless, the users have no control over their data in this process. Certain aspects, such as communication and computation cost, nature of cloud and others, are not considered in existing approaches [31]. Owing to the rapid rise in the popularity and availability of cloud services, it is now possible to conveniently store data and make computations remotely at any time. However, to a large extent, the wider implementation of cloud technologies is strongly impeded by privacy and security concerns. Aside the security challenges associated with the use of cloud technology, the user's inability to directly control their computation or data stresses the need for new techniques to assess the accountability and transparency of service providers.

Cloud storage offers the service of remotely saving, managing, and maintaining data [32]. Through a network, like the Internet, users can get access to this service. It does not only enable users to save their files online, but it also allows them to retrieve such files from anywhere in the world through the internet. While using most of these services attracts no fee for a particular number of gigabytes, there is a monthly fee for extra storage. Drag-and-drop accessibility and synchronization of files and folders between the cloud drive, and your mobile devices and desktop are available in all cloud storage services. All of these services also allow users to team up to work on documents.

Since users have no control over the public cloud, this obviously makes it look risky [33]. From 2013 to 2014, the number of managers who cited security as a major challenge fell from 44% to 25%, as reported in the CIO Mid-Year Review of 2014, which is an Indian survey of CIOs [34]. Nevertheless, cloud computing gives cybercriminals a chance to steal users' data, especially through fierce denial-of-service attacks (Fig. 3).

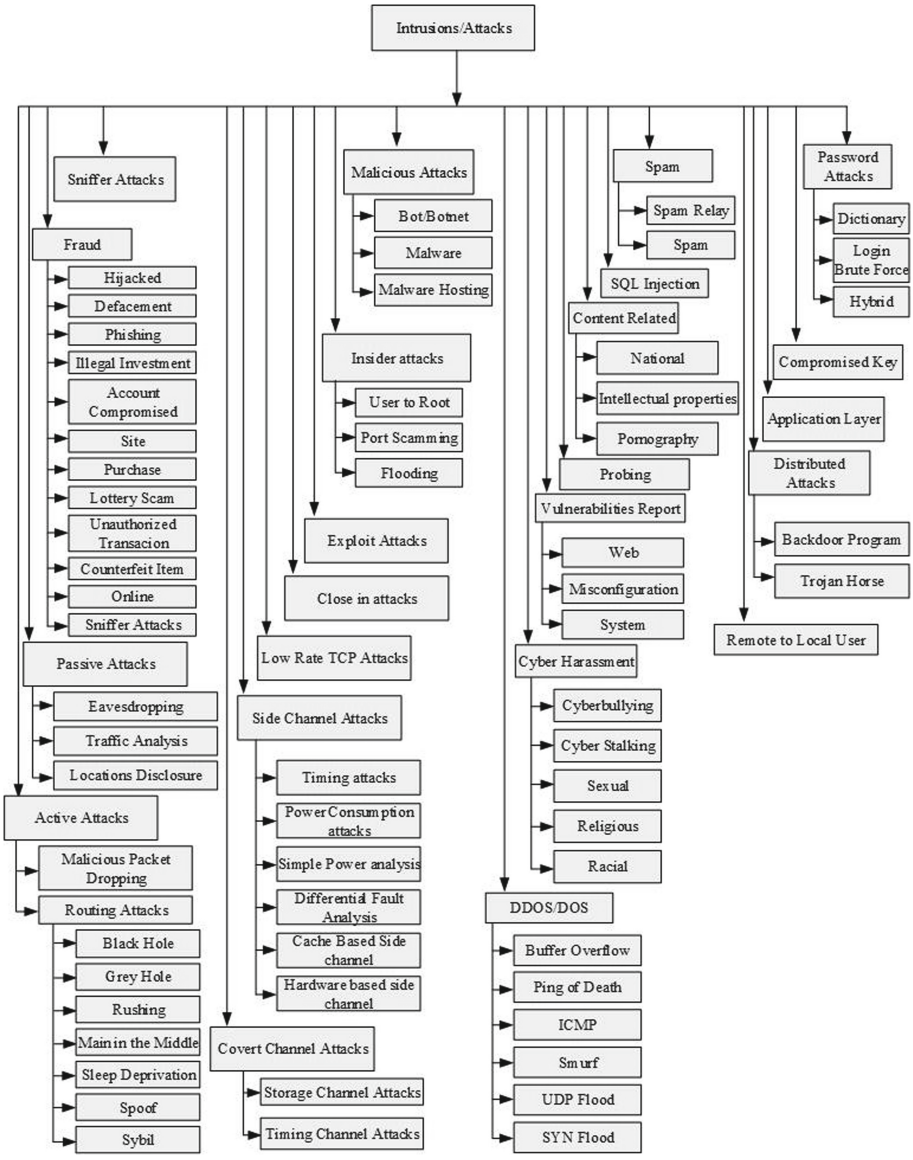

Fig. 3. Complete list of intrusions/attacks

2.1 DDoS Attacks

A DDoS attack capitalizes on the distributiveness of the Internet, with disparate entities owning hosts across the globe [37]. A DDoS attacker tries to utilize the backbone network to disseminate various forms of DDoS attacks to the target network. Afterwards, a myriad of Zombies, representing passive and active

attackers, are built by the attacker [38]. A user is then exposed to DDoS attack. Figure 4 demonstrates the applicability of this attack mechanism to every type of computer network.

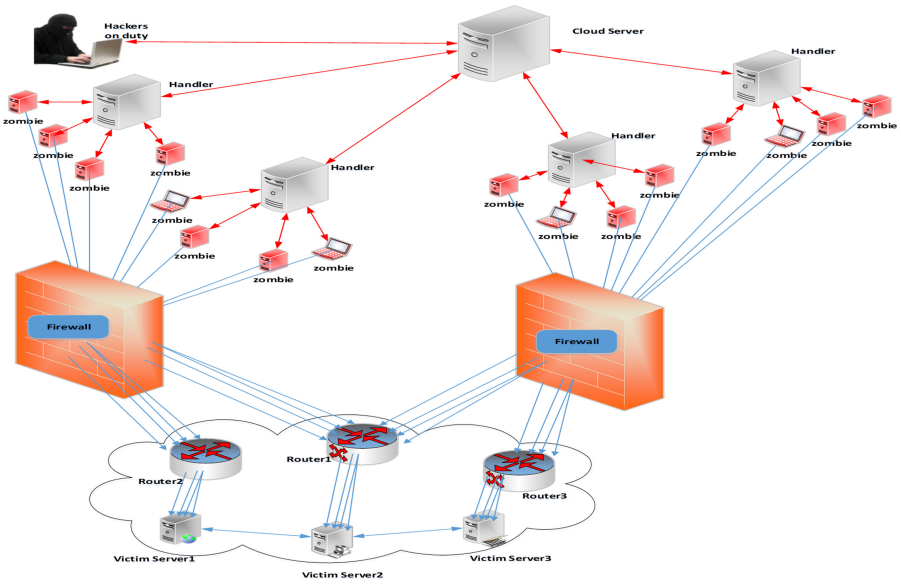

Fig. 4. DDoS attack

The below Table 1 describes the attack types of the DDoS

Table 1. DDoS attack types

DDoS Attack	DDoS characteristics and types			
	Infrastructure	Application	Direct	Reflection
UDP flood	✓	✓	✓	✓
TCP flood	✓		✓	
HTTP flood	✓	✓	✓	
ICMP flood	✓		✓	
XML flood		✓	✓	
Ping of death	✓	✓		
Smurf	✓			✓

UDP (User Datagram Protocol) is a protocol that requires no connection. The receiver and sender do not need to exchange handshake when using UDP

to send data packets [49]. Packets will get to the receiver for processing. The victim's system may become saturated when numerous packets are sent. As a result, genuine users on the system would be deprived of adequate bandwidth. Specific or any ports on the victim's system will be sent UDP packets when the attacker floods their system with UDP attacks [50].

In the meantime, the application that forwards the request should be identified by the system [51]. The victim's system would signal that the destination is not accessible by sending out ICMP packet if the targeted port has no running applications [52]. Like smurfing, spoofed IP address is used in UDP flooding to send the attacking packet [53]. The spoofed address helps to ensure that return packets are not forwarded back to the zombie system, but to another system entirely [54]. As seen in Fig. 5, UDP flood attacks can cause connectivity problems in the victim's system by saturating their bandwidth connection.

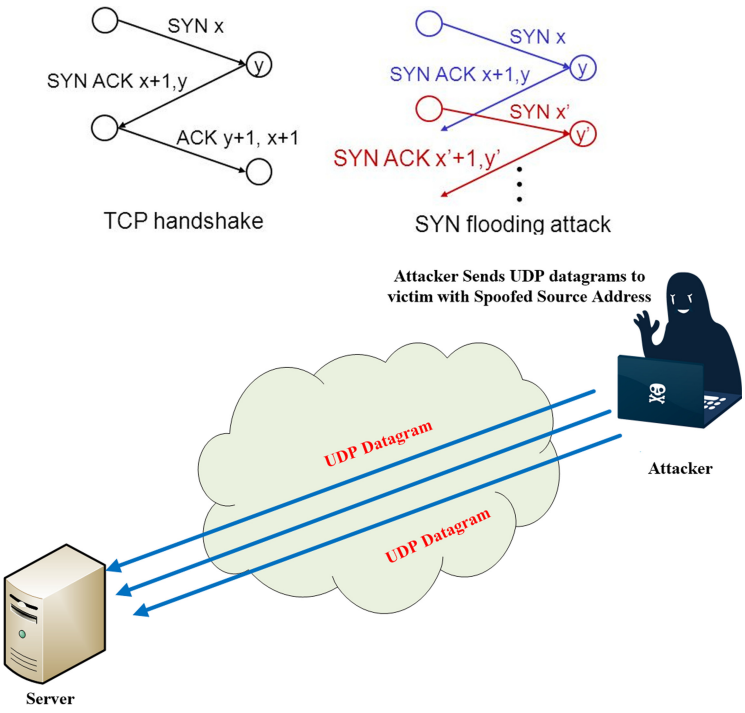

Fig. 5. UDP flooding attack

Another form of a Dos/DDoS attack is the TCP SYC attack where the three-way handshake is deliberately violated by the attacker to open various half-opened IP/TCP connections [55]. Internet-connected systems providing TCP-based network services are the possible targets of this attack. Mail server, FTP server, and web server are some examples [56]. A series of messages referred

to as the three-way handshake are exchanged between a server (i.e., a system offering a service) and a client when a TCP connection is established with the server. The server then get a Synchronization Message from the Client's system [57]. In return, the client receives the SYN-ACK message from the server and replies to it with an ACK message. After an acknowledgment has been sent by the server system, there will be a problem if the client fails to receive the final ACK message [58].

Moreover, there is an in-built data structure in the server that describes all unfinished connections. The size of this data structure is finite, and the creation of many partially opened connections can make it overflow. The memory and processor resources of a server will be exhausted when the server is processing a huge volume of SYN requests and no single ACK-SYN response is acknowledged. During a TCP SYN attack, zombies are instructed to forward fake TCP SYN requests to the server of the victim in order to consume the processor resources of the server. This prevents legitimate requests from getting responses from the server. The attacker's identity is hidden, since the attacker uses a spoofed address in sending the SYN packet [59]. Figure 6 shows a normal and healthy TCP before and after attack.

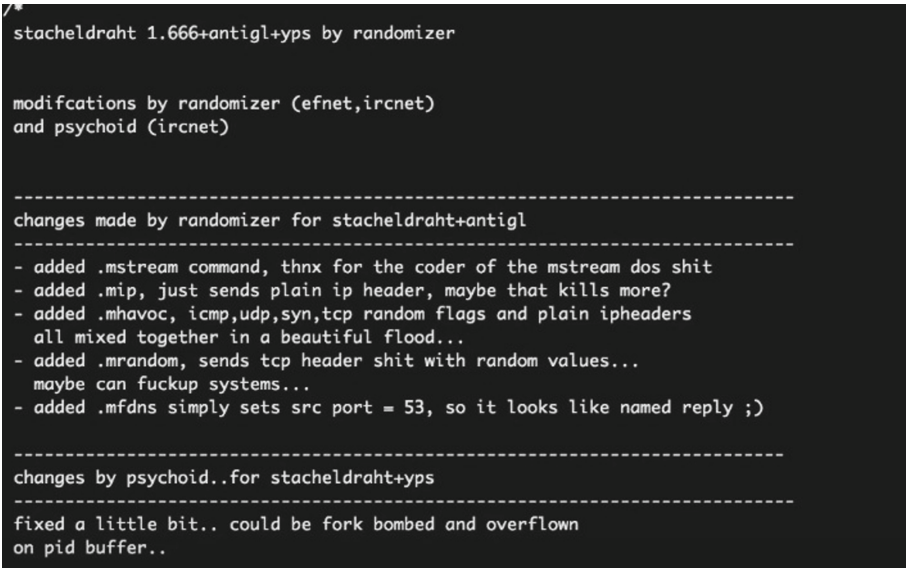

Fig. 6. TCP SYN flood attacks Source: Incapsula (2017).

Genuine traffic and attack traffic can be generated using several tools [60]. These days, it has been found that botnets are used in launching all DDoS attacks. So far, no detailed solution has been formulated to address these DDoS attacks. The development of a more effective solution is hindered by the lack of

in-depth comparison between traffic generators and basic technical components of DDoS attack devices. DDoS attack devices are usually structured to cause a traffic jam at the terminal level congestion at the server of the victim, or at the connection level congestion at the network of the victim.

The C-based DDoS device for creating Smurf, UDP flood, SYN flood and ICMP flood attack towards the target is called Stacheldraht [60]. It is capable of spoofing the IP address and congesting the link. Its execution is supported on both Solaris Version 2.1 and Linux. The command-line-based interface is shown in Fig. 7, where an agent-based flood network serves as the DDoS attack tool.

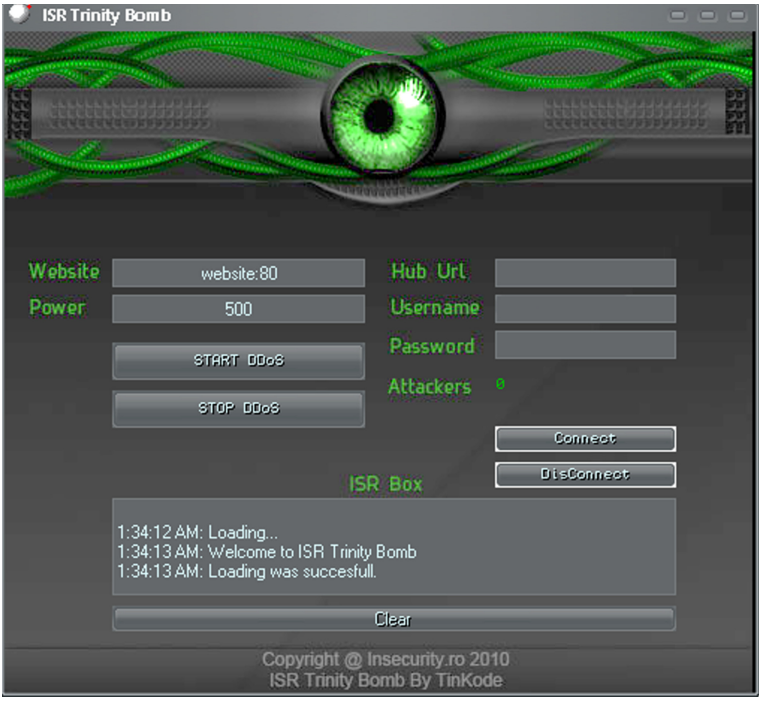

Fig. 7. Stacheldraht DDoS command-line tool Source: Barga (2010) [61]

Null, flags, random, RST, SYN, fragment and UDP flood requests, which cause link congestion and exhaustion of end-point resources, can be launched using a command-line based attack device known as Trinity [62]. As shown in Fig. 8, Trinity requires Linux platform and utilizes the encrypted format, while its architectural model is based on IRC.

This attack tool is based on C, and its underlying execution platform is Windows, Unix or Linus [64]. It used to cause the crash of Windows 2000 machine by sending numerous random port numbers and random IP addresses (i.e., TCP packets with arbitrary settings) to exploit and increase the machine load. It has

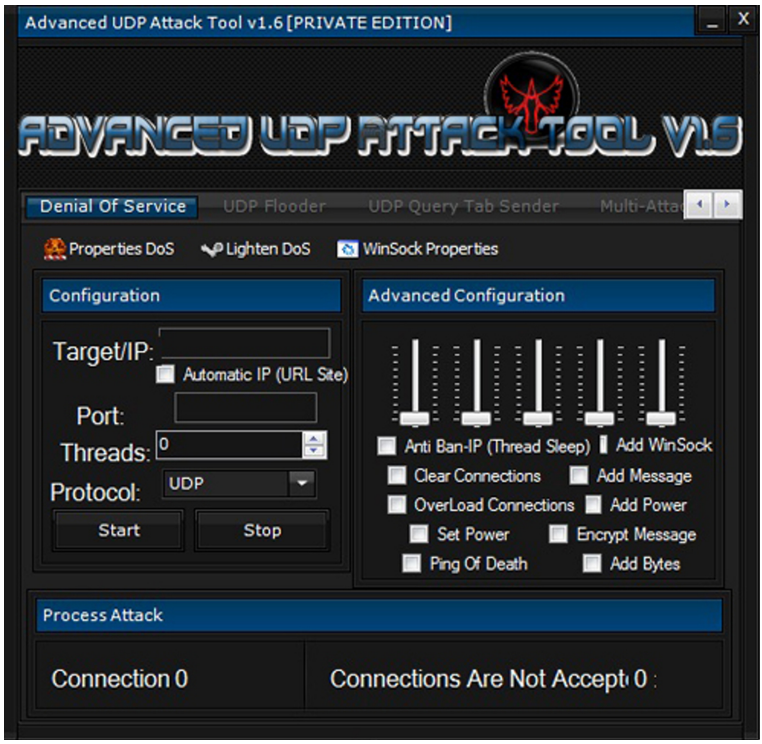

Fig. 8. Trinity DDoS traffic generating tool Source: Stuff (2017) [63]

a command-line interface and is built on C. It also has the capacity to fabricate the source addresses [65], and can direct both TCP RST flood and TCP ACK flood requests at the victim's server. It is able to create botnets and hide the attackers' IP addresses, as well as carry out DDoS attacks. The bandwidth and network resources of the target server can be exhausted by both requests.

Another DDoS attack device, with command line interface, that can consume the resources and bandwidth of the target server is Shaft [66]. It chooses whether or not to terminate the zombies (aside attacking), assists the attackers in identifying the status of the target machine (either alive or totally down), and gives statistics for ICMP, UDP and TCP flooding attacks. The architecture model of this attack tool is based on Agent Handler.

UDP Unicorn is a Win32 UDP flooding DDoS tool that has a multithreading ability. UDP sockets are created using Winsock, and are employed in flooding a target to test network security [67]. Figure 2.15 shows the graphic interface for this tool, which is widely used nowadays. LOIC-IFC was created by the Indonesia Fighter Cyber hacking team. It has a different default UDP/TCP flood message that contains the Malay phrase "Merdeka atau Mati", which is interpreted in English as "Freedom or Death" [69]. Technically, it further increases the chances

of adding random characters to the packet payload for UDP/TCP, and to the attacked URL for HTTP flood. The interface of the LOIC-IFC tool is shown in Fig. 9.

Fig. 9. LOIC-IFC tools Source: Segal (2017) [70]

As seen in Table 1, identified key features are used in comparing all the prominent attack devices. Implementation language, support of operating systems, type of launched attack, scope of the attack device, and the impact of attack in reducing the resource or bandwidth level are some of these key features. In addition, the attack tool architecture of all DDoS attack tools has been observed to be similar.

2.2 DDoS Datasets and Traffic Captures

Various network intrusion datasets have been introduced by several security research groups to examine different unknown attacks and intrusion detection techniques [71]. Network simulation datasets, private datasets and public datasets are the three categories into which these datasets are classified [72]. A large number of the private and public intrusion datasets have been generated using various tools. These tools are capable of monitoring traffic patterns, launching attacks of different kinds, pre-processing and capturing traffic, and

identifying victims. DARPA (Defence Advanced Research Projects Agency) is the agency responsible for developing new military technologies in the United State Department of defence [73]. All the datasets provided by DARPA are produced synthetically, and the rationale behind the underlying traffic models employed has been questioned. Furthermore, all the presented datasets were not recorded on an Internet-connected network. Many abnormal traffics that cannot be linked to any harmful behaviour are usually contained in Internet traffic, and such types of abnormalities might not be included in datasets recorded in an Internet-isolated network.

2.2.1 DDcup99

The KDD Cup 1999 is a benchmark dataset for detecting intrusion. A record, which contains 3 categorical attributes and 38 numeric discrete and numeric continuous attributes, is used to represent the connection between two host networks in this dataset [74]. Each record is either labelled as a specific or a normal type of attack. There are four categories of attacks, which include Probe, U2R (User to Root), R2L (Remote to Local) and DoS/DDoS [75].

2.2.2 SL-KDD

NSL-KDD is an intrusion dataset that is based on a network. It is a refined form of the intrusion detection benchmark dataset of KDD Cup 1999 produced from the same testbed [76]. The dataset of KDD Cup 1999 has several instances that are unimportant and may be biased in its learning processes towards repeated records. This problem is solved by keeping just one of the duplicated records in the NSL-KDD dataset [77].

2.2.3 CAIDA

In this dataset, there are about 60 min of unknown traffic traces that occurred on August 4, 2007 due to a DDoS attack [78]. Both the bandwidth of the network that connects the server to the web and the server's computing resources are consumed in this type of denial-of-service attack, and this makes the targeted server inaccessible. The 60-minute trace is divided into several PCAP files of 5 min [79]. The dataset has an uncompressed size of 21 GB and a comprised size of 5.3 GB. The traces only include attacks directed at the victim and the victim's responses to the attacks [80]. Serious efforts have been made to minimize the inclusion of non-attack traffic. All packets have been cleared of the payload. Any software, such as Wireshark, TCPDUMP and Coral Reef Software Suite, that can read the TCPDUMP (PCAP) format can also read these traces.

2.2.4 TUIDS

Tezpur University researchers have collected the TUIDS dataset [81]. By making use of a laboratory in which isolated networks were established, various tasks for extracting features from flow data and network packet were involved in generating the dataset. Attacks were generated against a local network host or

server using existing attack tools, and the generated traffic, which is referred to as attack traffic, was then collected [82]. Depending on the attack distribution, characteristics and the type employed, TUIDS datasets were classified into:

- Portscan.
- Network flow traffic feature dataset.
- Packet traffic feature dataset.

The extracted features determine the dataset dimensionalities. Researchers have reported some attributes of these datasets, the process of generating them, and testbed utilized in generating them. Forty nodes, two workstations, one server, one router, one L3 switch, and two L2 switches were included in the testbed for capturing the network traffic. Six VLANs were produced using the L2 and L3 switches, and the VLANs were separated by connecting workstations and nodes. An internal IP router was connected to the L3 switch, and an external IP router was used to connect the router to the Internet.

As shown in Fig. 10, the traffic observation activity of the switch, the server was connected to the L3 switch through a mirror port. Another LAN of 350 nodes was connected to other VLANs through five L3 and L2 switches and three routers. The attacks were launched within the testbed as well as from another LAN through the Internet. To launch attacks within the testbed, nodes of one VLAN were attacked from nodes of another VLAN as well as the same VLAN. Normal traffic was created within the testbed in a restricted manner after disconnecting the other LAN. Traffic activities in the testbed were observed on the computer connected to the mirror port.

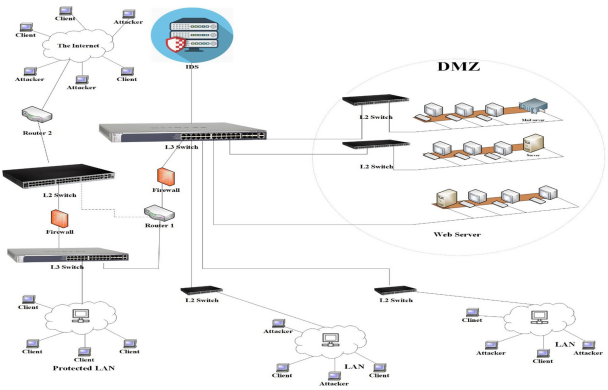

Fig. 10. TUIDS dataset testbed generation Mitigation Method for DDoS Source: Bhuyan et al. (2015)

Kazemi et al., used signature-based and genetic-based techniques for intrusion detection [132]. Their cloud intrusion detection datasets can detect cloud attacks as shown in Fig. 2.30. Cloud-based IDSs could detect 94% of random sets

of cloud attacks. By adding the background traffic retrieved from DARPA, IDS could detect the same amount of attacks and no false positive alarm was raised while filtering the background traffic.

Annappaian and Agrawal have a technique called cloud service usage profile based on IDPS was developed by [133]. This technique can detect and prevent intruders in cloud service intrusion based on the cloud service usage profile as shown in Fig. 2.31. In addition, this usage profile helps to detect unusual usage and prevent intrusion. This profile-based IPS gives active response to intruder/vendor by updating policies and signatures. It also modifies the destination entity that was attempted for attack. The cloud vendor can view the logs and records provided by the honey pot recorded system to take safety action in the future. The example below shows the usage profile based on IDPS.

Ramteke et al., proposed an open source security event correlator for H-IDPS; however, the effectiveness of their work is not clear [134]. In addition, their work did not make use of features because they depended only on a real-time virtual machine in Fig. 2.32. In their study, a new intrusion detection called FCANN technique was proposed based on ANN and fuzzy clustering. Through the fuzzy clustering technique, the heterogeneous training set was divided into several homogenous subsets. Thus, the complexity of each sub training set was reduced and consequently the detection performance increased.

In Bhat et al., a machine learning techniques such as the NB tree and random forest were implemented to detect intrusions in virtual machine environments of the cloud [135]. First, the NB tree was used for anomaly detection. Then, the NB tree and the random forest were used as hybrid classification for balanced dataset. Also, it builds intrusion patterns from a balanced training dataset and classifies the captured network connections from VMM to the main types of intrusions owing to the built patterns. They implemented the system in JAVA using the NB tree original implementation and tested it using the NSL-KDD of KDD'99 datasets as shown in Fig. 2.33. The random forest was used as a data mining classification algorithm in their proposed unsupervised anomaly detection method to partition the captured network connections from VMM. It was then used to pre-process specified number of features and detect the anomalous event depending on their features.

The proposed detection algorithm by Kumar P.A.R. and Selvakumar dealt with both discrete and continuous attributes in the database, which is practically useful for real-time network datasets [136]. The main objective of their study was to provide an efficient false positive reduction technique to minimize false alarms which demonstrate in Fig. 2.34. The NFBoost algorithm proposed in the study demonstrates the use of the Neyman Pearson technique as a post-training step to minimize the cost of misclassification errors.

Each technique has its own limitations and advantages (see Tables 2 and 3) that affect the accuracy and efficiency of H-IDPS.

Table 2. HIDPS advantages and limitations

IDS/H-IDPS technique	Characteristics/Advantages	Limitations/Challenges
Detection of misuse	• Use pre-configured knowledge base to match patterns and detect intrusions • Small computational cost • Big accuracy in detection of known attacks	• Cannot detect unknown variants of known attacks • The base of knowledge that is used for matching needs to be designed carefully • High rate of false alarms for unknown attacks
Anomaly detection	• Uses statistical test on collected behavior to identify intrusions • Can reduce the rate of false alarms for unknown attacks	• Requires a lot of time to identify attacks • Detection accuracy is based on the amount of collected behaviour features
H-IDPS based on Fuzzy logic	• Used for quantitative features • Provides better flexibility to some uncertain problems	• It has a lover detection accuracy than ANN
ANN based H-IDPS	• Classifies unstructured network packets, efficiently • ANN efficiency of classification is increased when there is a use of Multiple hidden layers	• Needs a lot of time and large number of training examples • It needs big number of samples to train effectively • Has low flexibility
SVM based H-IDPS	• Although the sample data is limited it can still correctly classify intrusions • It can manage a massive number of features	• Classifies only discrete features. So, before applying there is a need of pre-processing of that feature
H-IDPS based on association rules	• Used to detect signatures of relevant known attacks in misuse detection	• Not useful for unknown attacks • Needs a lot of database scans to generate rules • It can be used only for misuse detection
GA based H-IDPS	• Used to select best detection features • Has high level of efficiency	• Complex method. Used in specific way rather than general
Hybrid techniques	• Efficient approach for accurate classification	• It has a high computational cost

Table 3. The most critical H-IDPS summarization

Author(s)	Methodology	Description	Strengths and weaknesses
[1]	Fuzzy C Means clustering algorithm and Artificial Neural Network(FCM-ANN)	Improve the accuracy of the detection system	Strengths: They proposed system can detect the anomalies with high detection accuracy and low false alarm rate even for low frequent attacks Weaknesses: The major drawbacks of both underlying systems are thus need more investigate. However, their proposed leak on the limitation of detection low false alarm rate, Remote to Local (R2L) and User to Root (U2R)
[3]	Fuzzy logic can be set with predefined rules by which it can detect the malicious packets and takes proper counter measures to mitigate the DDoS attack	Fuzzy Inference System based defence mechanism that use for real time traffic analysis. Signature pattern database is built from supervised and unsupervised learning method	Strengths: A fuzzy logic based defence mechanism that is first trained with training data and rules are defined as per the possible traffic pattern of the cloud environment Weaknesses: Less Significant training time can restrict it to be used in dynamic network
[5]	They have developed N-IDPS	Component in cloud computing system which uses Snort and signature Apriori algorithm	Strengths: emphasized the usage of alternative options to incorporate intrusion detection or intrusion prevention techniques into Cloud and explored locations in Cloud where H-IDPS can be positioned for efficient detection and prevention of intrusion Weaknesses: The N-IDPS may become the target of an attack itself. An attacker may utilize techniques to reduce the ability of the N-IDPS to detect an attack to allow the attacker to slip their traffic though undetected
[6]	Multi-threaded N-IDPS model for distributed cloud environment	A multi-threaded cloud IDS models proposed which can be administered by a third-party monitoring service fora better optimized efficiency and transparency for the cloud user	Strengths: High volume of data in cloud environment could be handled by a single node N-IDPS through a multi-threaded approach Weaknesses: Third party monitoring and advisory service are costly

3 Summary

The distributed and open structure of cloud computing and services becomes an attractive target for potential cyber-attacks by intruders. IDPS are largely inefficient to be deployed in cloud computing environments due to their openness and specific essence. IDPS in cloud computing as any exciting system needs to be improved and in this article, discusses IDS and IPS, the threats that H-IDPS are trying to catch, the myths behind these two systems, the challenges that H-IDPS face and the types of alerts that H-IDPS triggers. Also, in this

article briefing know the state of art stage that the H-IDPS reaches, it can start from that point to build our research. By the finding of this article our finding came out with: A proof that H-IDPS in DDoS cloud are not the same system. The type of threats is defined and categorized. In future work will focus in COVID-19, which contagion has brought in extraordinary and special social and financial conditions leveraged by cyber-crime. Thus, a new modern mechanism should proposed for the IDS/IPS in cloud computing through the pandemic cybersecurity attacks. There is a lack of researches to cover H-IDPS true positive alerts and true negative alerts over cloud DDoS attack, which next article address an overcome this issue.

References

1. Pandeeswari, N., Kumar, G.: Anomaly detection system in cloud environment using fuzzy clustering based ANN. Mobile Netw. Appl. **21**, 1–12 (2015)
2. Rittinghouse, J.W., Ransome, J.F.: Cloud Computing: Implementation, Management, and Security. CRC Press, Boca Raton (2016)
3. Iyengar, N.C.S., Banerjee, A., Ganapathy, G.: A fuzzy logic based defense mechanism against distributed denial of service attack in cloud computing environment. Int. J. Commun. Netw. Inf. Secur. **6**(3), 233 (2014)
4. Kaul, S., Sood, K., Jain, A.: Cloud computing and its emerging need: advantages and issues. Int. J. Adv. Res. Comput. Sci. **8**(3) (2017)
5. Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., Rajarajan, M.: A survey of intrusion detection techniques in cloud. J. Netw. Comput. Appl. **36**(1), 42–57 (2013)
6. Shelke, M.P.K., Sontakke, M.S., Gawande, A.: Intrusion detection system for cloud computing. Int. J. Sci. Technol. Res. **1**(4), 67–71 (2012)
7. Armbrust, M., et al.: A view of cloud computing. Commun. ACM **53**(4), 50–58 (2010)
8. Zhang, Q., Cheng, L., Boutaba, R.: Cloud computing: state-of-the-art and research challenges. J. Internet Serv. Appl. **1**(1), 7–18 (2010)
9. Qian, L., Luo, Z., Du, Y., Guo, L.: Cloud computing: an overview. In: Jaatun, M.G., Zhao, G., Rong, C. (eds.) CloudCom 2009. LNCS, vol. 5931, pp. 626–631. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10665-1_63
10. Iqbal, M., Dagiuklas, A.: Infrastructure as a Service (IaaS): a comparative performance analysis of open-source cloud platforms. In: The International Workshop on Computer-Aided Modeling Analysis and Design of Communication Links and Networks (CAMAD), Lund, Sweden (2017)
11. Rodriguez, M.A., Buyya, R.: A taxonomy and survey on scheduling algorithms for scientific workflows in IaaS cloud computing environments. Concurrency Comput. Pract. Exp. **29**(8) 2017
12. Piraghaj, S.F., Dastjerdi, A.V., Calheiros, R.N., Buyya, R.: A survey and taxonomy of energy efficient resource management techniques in platform as a service cloud. In: Handbook of Research on End-to-end Cloud Computing Architecture Design, pp. 410–454 (2017)
13. Ren, L., Zhang, L., Wang, L., Tao, F., Chai, X.: Cloud manufacturing: key characteristics and applications. Int. J. Comput. Integr. Manuf. **30**(6), 501–515 (2017)

14. Loganayagi, B., Sujatha, S.: Enhancing cloud security through policy monitoring techniques. In: Das, V.V., Thankachan, N. (eds.) CIIT 2011. CCIS, vol. 250, pp. 270–275. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25734-6_40
15. Jaber, A.N., Rehman, S.U.: FCM–SVM based intrusion detection system for cloud computing environment. Cluster Comput. **23**(4), 3221–3231 (2020). https://doi.org/10.1007/s10586-020-03082-6
16. Jaber, A.N., Zolkipli, M.F., Shakir, H.A., Jassim, M.R.: Host based intrusion detection and prevention model against DDoS attack in cloud computing. In: Xhafa, F., Caballé, S., Barolli, L. (eds.) 3PGCIC 2017. LNDECT, vol. 13, pp. 241–252. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-69835-9_23
17. Jaber, A.N., Zolkipli, M.F., Majid, M.A., Anwar, S.: Methods for preventing distributed denial of service attacks in cloud computing. Adv. Sci. Lett. **23**(6), 5282–5285 (2017)
18. Contoli, C.: Virtualized Network Infrastructures: Performance Analysis, Design and Implementation. Alma (2017)
19. Oppitz, M., Tomsu, P.: Managing virtual storage. Inventing the Cloud Century, pp. 131–138. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-61161-7_6
20. Perez-Botero, D., Szefer, J., Lee, R.B.: Characterizing hypervisor vulnerabilities in cloud computing servers. In: Proceedings of the 2013 International Workshop on Security in Cloud Computing, pp. 3–10. ACM (2013)
21. Kizza, J.M.: Virtualization technology and security. Guide to Computer Network Security. TCS, pp. 459–476. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-38141-7_21
22. Curtis, P.M., Cochran, M.J., Considine, J.F., Clarke, K.J.: Virtual network device in a cloud computing environment, ed: Google Patents (2017)
23. Blenk, A., Basta, A., Reisslein, M., Kellerer, W.: Survey on network virtualization hypervisors for software defined networking. IEEE Commun. Surv. Tutor. **18**(1), 655–685 (2016)
24. Cardente, J., Durazzo, K., Harwood, J.: Classification techniques to identify network entity types and determine network topologies, ed: Google Patents (2017)
25. Sheinidashtegol, P., Galloway, M.: Performance impact of DDoS attacks on three virtual machine hypervisors. In: 2017 IEEE International Conference on Cloud Engineering (IC2E), Vancouver, BC, Canada, 2017, pp. 204–214. IEEE, 11 May 2017
26. Freet, D., Agrawal, R., Walker, J.J., Badr, Y.: Open source cloud management platforms and hypervisor technologies: a review and comparison. In: Southeast-Con, pp. 1–8. IEEE (2016)
27. Celesti, A., Mulfari, D., Fazio, M., Puliafito, A., Villari, M.: Evaluating alternative DaaS solutions in private and public OpenStack Clouds. Soft. Pract. Exp. **47**, 1185–1200 (2017)
28. Deka , G.C., Das, P.K.: Application of virtualization technology in IaaS cloud deployment model. In: Design and Use of Virtualization Technology in Cloud Computing, p. 29 (2017)
29. Whitman, M.E., Mattord, H.J.: Threats to information protection-industry and academic perspectives: an annotated bibliography. J. Cybersecur. Educ. Res. Pract. **2016**(2), 4 (2016)
30. Li, Y., Gai, K., Qiu, L., Qiu, M., Zhao, H.: Intelligent cryptography approach for secure distributed big data storage in cloud computing. Inf. Sci. **387**, 103–115 (2017)

31. Naser, A., Majid, M.A., Zolkipli, M.F., Anwar, S.: Trusting cloud computing for personal files. In: International Conference on Information and Communication Technology Convergence (ICTC), vol. 2014, pp. 488–489 (2014)
32. More, S., Chaudhari, S.: Third party public auditing scheme for cloud storage. Procedia Comput. Sci. **79**(Suppl. C). 69–76 (2016)
33. Jaber, A.N., Zolkipli, M.F.B., Majid, M.B.A.: Security everywhere cloud: an intensive review of DoS and DDoS attacks in cloud computing. J. Adv. Appl. Sci. (JAAS) **3**(5), 152–158 (2015)
34. Himmel, M.A., Grossman, F.: Security on distributed systems: cloud security versus traditional IT. IBM J. Res. Dev. **58**(1), 3:1–3:13 (2014)
35. Nanavati, M., Colp, P., Aiello, B., Warfield, A.: Cloud security: a gathering storm. Commun. ACM **57**(5), 70–79 (2014)
36. Gillman, D., Lin, Y., Maggs, B., Sitaraman, R.K.: Protecting websites from attack with secure delivery networks. Computer **48**(4), 26–34 (2015)
37. Zlomislić, V., Fertalj, K., Sruk, V.: Denial of service attacks, defences and research challenges. Cluster Comput. **20**(1), 661–671 (2017). https://doi.org/10.1007/s10586-017-0730-x
38. Kamatchi, R., Ambekar, K., Parikh, Y.: Security mapping of a usage based cloud system. Netw. Protoc. Algorithms **8**(4), 56–71 (2017)
39. Akamai: Q2 2017 State of the Internet Security Report, Akamai, pp. 1–27, 30-6-2017 (2017)
40. Thomas, K., Invernizzi, L., Bursztein, E.: Understanding the Mirai Botnet (2017)
41. Zargar, S.T., Joshi, J., Tipper, D.: A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Commun. Surv. Tutor. **15**(4), 2046–2069 (2013)
42. Idziorek, J., Tannian, M.F., Jacobson, D.: The insecurity of cloud utility models. IT Prof. **15**(2), 22–27 (2013)
43. Ficco, M., Palmieri, F.: Introducing fraudulent energy consumption in cloud infrastructures: a new generation of denial-of-service attacks. IEEE Syst. J. **11**, 460–470 (2015)
44. Ficco, M., Palmieri, F.: Introducing fraudulent energy consumption in cloud infrastructures: a new generation of denial-of-service attacks. IEEE Syst. J. **11**(2), 460–470 (2017)
45. Saied, A., Overill, R.E., Radzik, T.: Detection of known and unknown DDoS attacks using Artificial Neural Networks. Neurocomputing **172**, 385–393 (2016)
46. Freedman, A.T., Pye, I.G., Ellis, D.P.: Network Monitoring, Detection, and Analysis System, ed: Google Patents (2017)
47. Lotus, B.: Level 3®DDoS Mitigation (2017)
48. Bhardwaj, A., Subrahmanyam, G., Avasthi, V., Sastry, H., Goundar, S.: DDoS attacks, new DDoS taxonomy and mitigation solutions–a survey. In: 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), ITM (part of Centurion University Of Technology & Management) Village Alluri Nagar, 2016, pp. 793–798. IEEE (2016)
49. Postel, J.: User datagram protocol, 2070–1721 (1980)
50. Rosli, A., Taib, A.M., Ali, W.N.A.W.: Utilizing the enhanced risk assessment equation to determine the apparent risk due to user datagram protocol (UDP) flooding attack. Sains Humanika **9**(1–4) (2017)
51. Kaur, G., Saxena, V., Gupta, J.: Detection of TCP targeted high bandwidth attacks using self-similarity. J. King Saud Univ. Comput. Inf. Sci. **32**, 35–49 (2017)

52. Kumar, D.: DDoS attacks and their types. In: Network Security Attacks and Countermeasures, p. 197 (2016)
53. Suhasaria, P., Garg, A., Agarwal, A., Selvakumar, K.: Distributed denial of service attacks: a survey. Imperial J. Interdisc. Res. **3**(3) (2017)
54. Bhushan, K., Gupta, B.: Security challenges in cloud computing: state-of-art. Int. J. Big Data Intell. **4**(2), 81–107 (2017)
55. Bogdanoski, M., Toshevski, A., Bogatinov, D., Bogdanoski, M.: A novel approach for mitigating the effects of the TCP SYN flood DDoS attacks. World J. Modell. Simul. **12**(3), 217–230 (2016)
56. Arshadi, L., Jahangir, A.H.: An empirical study on TCP flow interarrival time distribution for normal and anomalous traffic. Int. J. Commun. Syst. **30**(1) (2017)
57. Aslan, M., Matrawy, A.: Could network view inconsistency affect virtualized network security functions? arXiv preprint arXiv:1707.05546 (2017)
58. Deore, S., Patil, A.: Survey denial of service classification and attack with protect mechanism for TCP SYN flooding attacks (2016)
59. Kavisankar, L., Chellappan, C., Poovammal, E.: Against spoofing attacks in network layer. In: Combating Security Breaches and Criminal Activity in the Digital Sphere, pp. 41–56. IGI Global (2016)
60. Behal, S., Kumar, K.: Characterization and comparison of DDoS attack tools and traffic generators: a review. IJ Netw. Secur. **19**(3), 383–393 (2017)
61. Braga, R., Mota, E., Passito, A.: Lightweight DDoS flooding attack detection using NOX/OpenFlow. In: IEEE Local Computer Network Conference, Denver, CO, USA, 2010, pp. 408–415. IEEE, 22 March 2011
62. Bhuyan, M.H., Bhattacharyya, D.K., Kalita, J.K.: A systematic hands-on approach to generate real-life intrusion datasets. Network Traffic Anomaly Detection and Prevention. CCN, pp. 71–114. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-65188-0_3
63. Stuff, S.: Huburile si DDOS-ul (2011)
64. Kaur, H., Behal, S., Kumar, K.: Characterization and comparison of distributed denial of service attack tools. In: 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Denver, CO, USA, pp. 1139–1145. IEEE (2015)
65. Nagpal, B., Sharma, P., Chauhan, N., Panesar, A.: DDoS tools: classification, analysis and comparison. In: 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, pp. 342–346. IEEE (2015)
66. Kumar, V., Kumar, K.: Classification of DDoS attack tools and its handling techniques and strategy at application layer. In: 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall), Bareilly, India, pp. 1–6. IEEE (2016)
67. Somal, L., Virk, S.: Classification of distributed denial of service attacks–architecture, taxonomy and tools. Int. J. Adv. Res. Comput. Sci. Technol. **2**(2), 118–122 (2014)
68. HARIS: Understanding DDoS (2016)
69. Segal, L.: Thanks to Anonymous' Latest Toolset, Anyone Can Play the DDoS Game (2016)
70. Segal, L.: Anonymous DDOS Tools 2016 (2017)
71. Behal, S., Kumar, K.: Trends in validation of DDoS research. Procedia Comput. Sci. **85**, 7–15 (2016)
72. Singh, J., Kumar, K., Sachdeva, M., Sidhu, N.: DDoS attack's simulation using legitimate and attack real data sets. Int. J. Sci. Eng. Res. **3**(6), 1–5 (2012)

73. Maher, M., Smith, A., Margiotta, J.: A synopsis of the Defense Advanced Research Projects Agency (DARPA) investment in additive manufacture and what challenges remain. In: Laser 3D Manufacturing, vol. 8970, p. 897002. International Society for Optics and Photonics (2014)
74. Kohavi, R., Brodley, C.E., Frasca, B., Mason, L., Zheng, Z.: KDD-Cup 2000 organizers' report: peeling the onion. ACM SIGKDD Explor. Newslett. **2**(2), 86–93 (2000)
75. Davis, J.J., Clark, A.J.: Data preprocessing for anomaly based network intrusion detection: a review. Comput. Secur. **30**(6), 353–375 (2011)
76. Ingre, B., Yadav, A.: Performance analysis of NSL-KDD dataset using ANN. In: 2015 International Conference on Signal Processing and Communication Engineering Systems, Guntur, India, pp. 92–96. IEEE (2015)
77. Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A.A.: A detailed analysis of the KDD CUP 99 data set. In: 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, pp. 1–6. IEEE (2009)
78. Robinson, R.R., Thomas, C.: Ranking of machine learning algorithms based on the performance in classifying DDoS attacks. In: 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS), Trivandrum, India, pp. 185–190. IEEE (2015)
79. Grossman, R.L., Gu, Y., Sabala, M., Zhang, W.: Compute and storage clouds using wide area high performance networks. Future Gener. Comput. Syst. **25**(2), 179–183 (2009)
80. Singh, K., Singh, P., Kumar, K.: Application layer HTTP-GET flood DDoS attacks: research landscape and challenges. Comput. Secur. **65**, 344–372 (2017)
81. Bhuyan, M.H., Bhattacharyya, D., Kalita, J.K.: An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. Pattern Recogn. Lett. **51**, 1–7 (2015)
82. Bhatia, S., Schmidt, D., Mohay, G., Tickle, A.: A framework for generating realistic traffic for Distributed Denial-of-Service attacks and Flash Events. Comput. Secur. **40**, 95–107 (2014)
83. Tjhai, G.C., Papadaki, M., Furnell, S.M., Clarke, N.L.: The problem of false alarms: evaluation with Snort and DARPA 1999 dataset. In: Furnell, S., Katsikas, S.K., Lioy, A. (eds.) TrustBus 2008. LNCS, vol. 5185, pp. 139–150. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85735-8_14
84. Li, H., Liu, B., Mukherjee, A., Shao, J.: Spotting fake reviews using positive-unlabeled learning. Computación y Sistemas **18**(3), 467–475 (2014)
85. Witten, I.H., Frank, E., Hall, M.A., Pal, C.J.: Data Mining: Practical machine learning tools and techniques. Morgan Kaufmann, Burlington (2016)
86. Salman, T., Bhamare, D., Erbad, A., Jain, R., Samaka, M.: Machine learning for anomaly detection and categorization in multi-cloud environments. In: 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 97–103. IEEE (2017)
87. Chatterjee, T., Bhattacharya, A.: VHDL modeling of intrusion detection & prevention system (IDPS) a neural network approach. arXiv preprint arXiv:1402.5275 (2014)
88. Xing, T., Huang, D., Xu, L., Chung, C.-J., Khatkar, P.: SnortFlow: a openflow-based intrusion prevention system in cloud environment. In: 2013 Second GENI Research and Educational Experiment Workshop, pp. 89–92. IEEE (2013)
89. Bharot, N., Verma, P., Sharma, S., Suraparaju, V.: Distributed denial-of-service attack detection and mitigation using feature selection and intensive care request processing unit. Arab. J. Sci. Eng. **43**, 959–967 (2017)

90. Purwanto, Y., Rahardjo, B.: Traffic anomaly detection in DDos flooding attack. In: 2014 8th International Conference on Telecommunication Systems Services and Applications (TSSA), pp. 1–6. IEEE (2014)
91. Douligeris, C., Mitrokotsa, A.: DDoS attacks and defense mechanisms: classification and state-of-the-art. Comput. Netw. **44**(5), 643–666 (2004)
92. Zudin, R.: Transport layer DDoS attack types and mitigation methods in networks (2015)
93. Ning, L., Sen, S., Maohua, J., Jian, H.: A router based packet filtering scheme for defending against DoS attacks. China Commun. **11**(10), 136–146 (2014)
94. Fallah, M.S., Kahani, N.: TDPF: a traceback based distributed packet filter to mitigate spoofed DDoS attacks. Secur. Commun. Netw. **7**(2), 245–264 (2014)
95. Kolahi, S.S., Alghalbi, A.A., Alotaibi, A.F., Ahmed, S.S., Lad, D.: Performance comparison of defense mechanisms against TCP SYN flood DDoS attack. In: 2014 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), St. Petersburg, Russia, pp. 143–147. IEEE (2014)
96. Hang, B., Hu, R.: A novel SYN Cookie method for TCP layer DDoS attack. In: International Conference on Future BioMedical Information Engineering, FBIE 2009, pp. 445–448. IEEE (2009)
97. Kavisankar, L., Chellappan, C.: A mitigation model for TCP SYN flooding with IP Spoofing. In: 2011 International Conference on Recent Trends in Information Technology (ICRTIT), pp. 251–256. IEEE (2011)
98. Mahale, V.V., Pareek, N.P., Uttarwar, V.U.: Alleviation of DDoS attack using advance technique. In: 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 172–176. IEEE (2017)
99. Firoozjaei, M.D., Jeong, J.P., Ko, H., Kim, H.: Security challenges with network functions virtualization. Future Gener. Comput. Syst. **67**, 315–324 (2017)
100. Chandramouli, R.: Security Recommendations for Hypervisor Deployment. US Department of Commerce, National Institute of Standards and Technology (2014)
101. Gupta, S., Kumar, P.: VM profile based optimized network attack pattern detection scheme for DDOS attacks in cloud. In: Thampi, S.M., Atrey, P.K., Fan, C.-I., Perez, G.M. (eds.) SSCC 2013. CCIS, vol. 377, pp. 255–261. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40576-1_25
102. Xiao, L., Xu, D., Xie, C., Mandayam, N.B., Poor, H.V.: Cloud storage defense against advanced persistent threats: a prospect theoretic study. IEEE J. Sel. Areas Commun. **35**(3), 534–544 (2017)
103. Abdlhamed, M., Kifayat, K., Shi, Q., Hurst, W.: Intrusion prediction systems. In: Alsmadi, I.M., Karabatis, G., AlEroud, A. (eds.) Information Fusion for Cyber-Security Analytics. SCI, vol. 691, pp. 155–174. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-44257-0_7
104. Ndibwile, J.D., Govardhan, A., Okada, K., Kadobayashi, Y.: Web server protection against application layer DDoS attacks using machine learning and traffic authentication. In: 2015 IEEE 39th Annual Computer Software and Applications Conference, vol. 3, pp. 261–267. IEEE (2015)
105. Modi, C.N., Acha, K.: Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review. J. Supercomputing **73**(3), 1192–1234 (2017)
106. Samarasinghe, S.: Neural Networks for Applied Sciences and Engineering: From Fundamentals to Complex Pattern Recognition. CRC Press, Boca Raton (2016)
107. Demuth, H.B., Beale, M.H., De Jess, O., Hagan, M.T.: Neural Network Design. Martin Hagan (2014)

108. Buibas, M., Izhikevich, E.M., Szatmary, B., Polonichko, V.: Neural network learning and collaboration apparatus and methods, ed: Google Patents (2017)
109. Tang, J., Deng, C., Huang, G.-B.: Extreme learning machine for multilayer perceptron. IEEE Trans. Neural Netw. Learn. Syst. **27**(4), 809–821 (2016)
110. Taud, H., Mas, J.F.: Multilayer perceptron (MLP). In: Camacho Olmedo, M.T., Paegelow, M., Mas, J.-F., Escobar, F. (eds.) Geomatic Approaches for Modeling Land Change Scenarios. LNGC, pp. 451–455. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-60801-3_27
111. Maren, A.J., Harston, C.T., Pap, R.M.: Handbook of Neural Computing Applications. Academic Press, Cambridge (2014)
112. Mukhopadhyay, I., Chakraborty, M., Chakrabarti, S., Chatterjee, T.: Back propagation neural network approach to Intrusion Detection System. In: 2011 International Conference on Recent Trends in Information Systems, pp. 303–308. IEEE (2011)
113. Corchado, E., Herrero, Á.: Neural visualization of network traffic data for intrusion detection. Appl. Soft Comput. **11**(2), 2042–2056 (2011)
114. Wang, G., Hao, J., Ma, J., Huang, L.: A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering. Expert Syst. Appl. **37**(9), 6225–6232 (2010)
115. Tsai, C.-F., Lin, C.-Y.: A triangle area based nearest neighbors approach to intrusion detection. Pattern Recogn. **43**(1), 222–229 (2010)
116. Horng, S.-J., et al.: A novel intrusion detection system based on hierarchical clustering and support vector machines. Expert Syst. Appl. **38**(1), 306–313 (2011)
117. Pawar, S.: Intrusion detection in computer network using genetic algorithm approach: a survey. Int. J. Adv. Eng. Technol. **6**(2), 730 (2013)
118. Khorshed, M.T., Ali, A.S., Wasimi, S.A.: A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Gener. Comput. Syst. **28**(6), 833–851 (2012)
119. Khalil, I.M., Khreishah, A., Azeem, M.: Cloud computing security: a survey. Computers **3**(1), 1–35 (2014)
120. Bhadauria, R., Chaki, R., Chaki, N., Sanyal, S.: A survey on security issues in cloud computing. IEEE Commun. Surv. Tutor. **71**, 1–15 (2011)
121. Farahmandian, S., Zamani, M., Akbarabadi, A., Moghimi, Y., Mirhosseini Zadeh, S.M., Farahmandian, S.: A survey on methods to defend against DDoS attack in cloud computing. System **6**(22), 26 (2013)
122. Arun, R.K.P., Selvakumar, S.: Distributed denial-of-service (DDoS) threat in collaborative environment-a survey on DDoS attack tools and traceback mechanisms. In: IEEE International Advance Computing Conference, IACC 2009, pp. 1275–1280. IEEE (2009)
123. Yang, L., Zhang, T., Song, J., Wang, J.S., Chen, P.: Defense of DDoS attack for cloud computing. In: 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE), vol. 2, pp. 626–629. IEEE (2012)
124. Vissers, T., Somasundaram, T.S., Pieters, L., Govindarajan, K., Hellinckx, P.: DDoS defense system for web services in a cloud environment. Future Gener. Comput. Syst. **37**, 37–45 (2014)
125. Wang, H., Jia, Q., Fleck, D., Powell, W., Li, F., Stavrou, A.: A moving target DDoS defense mechanism. Comput. Commun. **46**, 10–21 (2014)
126. Fujinoki, H.: Dynamic binary user-splits to protect cloud servers from DDoS attacks. In: Proceedings of the Second International Conference on Innovative Computing and Cloud Computing, p. 125. ACM (2013)

127. Tripathi, S., Gupta, B., Almomani, A., Mishra, A., Veluru, S.: Hadoop based defense solution to handle distributed denial of service (DDoS) attacks. J. Inf. Secur. **4**(3), 150 (2013)
128. Chapade, S., Pandey, K., Bhade, D.: Securing cloud servers against flooding based DDoS attacks. In: 2013 International Conference on Communication Systems and Network Technologies, pp. 524–528. IEEE (2013)
129. Martínez, C.A., Echeverri, G.I., Sanz, A.G.C.: Malware detection based on cloud computing integrating intrusion ontology representation. In: 2010 IEEE Latin-American Conference on Communications, pp. 1–6. IEEE (2010)
130. Zargar, S.T., Takabi, H., Joshi, J.B.: DCDIDP: a distributed, collaborative, and data-driven intrusion detection and prevention framework for cloud computing environments. In: 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Orlando, FL, USA, pp. 332–341. IEEE (2011)
131. Sharma, S., Gupta, A., Agrawal, S.: An intrusion detection system for detecting denial-of-service attack in cloud using artificial bee colony. In: Satapathy, S., Bhatt, Y., Joshi, A., Mishra, D. (eds.) Advances in Intelligent Systems and Computing, pp. 137–145. Springer, Singapore (2016). https://doi.org/10.1007/978-981-10-0767-5_16
132. Kazemi, S., Aghazarian, V., Hedayati, A.: Improving false negative rate in hypervisor-based intrusion detection in IaaS cloud. IJCAT Int. J. Comput. Technol. **2**(9), 348 (2015)
133. Annappaian, D.H., Agrawal, V.K.: Cloud services usage profile based intruder detection and prevention system: intrusion meter. Trans. Netw. Commun. **2**(6), 12–24 (2015)
134. Ramteke, S., Dongare, R., Ramteke, K.: Intrusion detection system for cloud network using FC-ANN algorithm. Int. J. Adv. Res. Comput. Commun. Eng. **2**(4) (2013)
135. Bhat, A.H., Patra, S., Jena, D.: Machine learning approach for intrusion detection on cloud virtual machines. Int. J. Appl. Innov. Eng. Manage. (IJAIEM) **2**(6), 56–66 (2013)
136. Kumar, P.A.R., Selvakumar, S.: Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems. Comput. Commun. **36**(3), 303–319 (2013)