A Review of Different DDOS Attacks in Cloud Based Environment

[1] Nivedita Bhardwaj*; [2] Anita Ganpati

[1] Assistant Professor, Department of Computer Science, St. Bede's College, Navbahar, Shimla

[2] Professor, Department of Computer Science, Himachal Pradesh University, Shimla

Corresponding Author: Nivedita Bhardwaj

Abstract: For different stakeholders to make an informed judgment about cloud adoption, security concerns pertaining to cloud computing are pertinent. In addition to data breaches, the attack space for cloud-specific solutions is being revisited by the cyber security research community since these problems impact service quality, budget, and resource management. One such severe attack in the cloud realm is the Distributed Denial of Service (DDoS) attack. It is merely a method of sending out countless fictitious requests to prevent actual users from accessing web resources. Some important data about the various kinds of DDoS assaults will be presented in this paper. The many DDoS varieties are compiled, along with their strike capabilities and, most importantly, how the best cloud computing environment issues can be addressed and resolved for the advantage of all cloud continuum stakeholders. The main obstacles to an efficient DDoS defense system are also examined.

Keywords: DDos, Botnet, cloud computing environment, online resources, and internet

Introduction

Data storage, computation, networking, and on-demand software resources are just a few of the services and computing resources that may be delivered in a flexible manner via the Internet using virtualization and credit goes to cloud computing (CC). Because of the CC's elastic nature, resources can be dynamically distributed as needed without requiring users to make significant investments in infrastructure and software licensing [1][2].

However, CC is vulnerable to security risks because of the same property that gives it flexibility. Attacks known as distributed denial of service (DDoS) are among the most dangerous threats. Although some study offers a thorough analysis of the aforementioned problem, illuminating HTTP flooding DDoS assaults in the CC environment as well as other DDoS attacks, the impact of DDoS attacks on CC has regrettably not been sufficiently studied [3].

The foundation of contemporary digital infrastructure is cloud computing, which provides more flexible and affordable options [4]. By allowing businesses to expand resources and improve operations in response to demand, these services open up advanced computing to a wider audience [5]. Smaller businesses may now compete in technology-driven marketplaces which has significant overhead and maintenance costs.

The cost economics of cloud computing, particularly with regard to infrastructure management as a single sector, is one of the major factors that influences this layer and has a wide-ranging effect on IT expenditure. This lowers the possibility of over- or under-provisioning by enabling demand-based resource allocation. This strategy aims to promote IT resource management at a rate that more closely matches operational requirements with consumer behavior, resulting in more sustainable IT consumption [6][7][8].

However, security problems like default key breaches and widespread illegal access highlight how crucial it is to use cloud threat prevention solutions. This is necessary to preserve sensitive data and to maintain cloud service providers' credibility with current or prospective clients [9].

Distributed Denial of Service (DDoS) attacks pose a hazard to cloud services and require sophisticated security measures to identify and counteract their persistent nature, failing which they may interfere with the cloud provider's ability to provide services.

Cloud computing has improved operational efficiency and scalability, but for stability and further development, security threats must be avoided. The cloud is essential to the entire digital economy, so it should be given top attention to continue evolving into a more secure platform. In the context of computer security, DDoS attacks remain a serious threat because they interfere with services by overloading a network with more traffic than it can effectively manage or that is necessary for regular operation, rendering the network inaccessible to all of its intended users [10][11][12].

This approach is centered on the deployment of botnets, which are networks of compromised devices that send large amounts of traffic to target systems in an attempt to interfere with their availability. Common methods for increasing traffic volume include amplification and reflection, which seriously jeopardize the integrity of network services [13].

The cloud environment may be more susceptible to DDoS assaults, for instance, when hackers use hacked computers as amplifiers or reflectors, which could result in massive traffic volumes that disrupt service stability and continuity [14][15][16].

Every defense must distinguish between harmful and legitimate packets. Furthermore, by identifying deviations from anticipated traffic behavior, anomaly-based systems can detect unknown attack vectors, including zero-day threats [17], while signature-based protection techniques use predetermined patterns to identify known threats. DL i.e. Deep Learning is an excellent tool for spotting fraudulent network traffic. Current DL-based algorithms are capable of successfully separating DDoS activity by learning intricate patterns from simple traffic data [18][19][20].

These models are utilized in many areas of cyber security, including secure data transfer, malware detection, and cloud data encryption, to mention a few, in addition to protecting against DDoS attacks. DL can be used to solve cybersecurity problems at both low-level abstractions because it can describe intricate, nonlinear, and hierarchical aspects [21][22].

Strong, flexible defenses are necessary due to the intricacy of cloud-based DDoS attacks. For these more complex attacks, DL offers dynamic cyber security solutions. DL-based techniques present viable ways to identify and stop DDoS attacks as they get more common and varied. [23]. However, to keep cloud service defenses effective, ongoing innovation is required. The foundation of DL is Deep Neural Networks (DNNs), which are made up of several processing layers that use nonlinear transformations to identify online threats[24][25].

This architecture, which is frequently employed in domains such as image recognition, is skilled at spotting minute variations in attack patterns—a feature that is essential for spotting DDoS attacks [26][27]. Indeed, in some cases, DL models have attained accuracy rates higher than 99%. Recent developments have improved the detection of cyber threats by handling unbalanced datasets effectively, such as Unsupervised Stacked Autoencoders (SAs) in conjunction with Decision Trees (DTs) [28][29].

Nevertheless, there are difficulties in applying DL to identify web-based assaults, even with its benefits. For example, the variety of web traffic makes it challenging to differentiate between dangerous and benign URLs. More research is needed to create systems that can recognize novel attack signatures and transform various URL types into formats appropriate for DL models [30][31].

Although there are many obstacles to overcome, using DL to lessen DDoS attacks in cloud systems has a lot of promise. Cloud infrastructures are especially susceptible to these kinds of attacks, and although DL provides tools for identifying intricate attack patterns, the sector encounters challenges like the dearth of extensive cloud-specific DDoS datasets and the requirement for transparent and explicable AI models[32][33]. Enhancing cloud-based defenses against complex assaults will require technological developments as well as a move toward responsible AI systems.

Bandwidth depletion attacks

Bandwidth depletion in a DDoS attack refers to flooding a target network (or its upstream links) with such a large amount of traffic that the available network bandwidth is saturated. As a result, legitimate traffic cannot reach (or is severely delayed reaching) the target because the attack traffic consumes (or “depletes”) the link capacity. This is a type of volumetric or flood-based DDoS attack [34].

Resource depletion based attacks

Aresource-depletion DDoS attackis a type of distributed denial of service attack in which the attacker’s goal is to exhaust critical computational or protocol resources of the victim system—such as CPU, memory, socket/connection state, buffer space, threads, or other finite system resources—rather than (or in addition to) saturating the network bandwidth. These attacks may exploit weaknesses in protocol implementations or force expensive operations per request, often using comparatively low traffic volume but high complexity per request [35].

Mixed Attacks/Advanced Emerging Attacks

Mixed attackscombine various attack vectors to increase effectiveness. For example, an attacker might use both volume-based and application-layer attacks simultaneously Unlike systems subject to only one single type of attacks (either DoS or FDI attacks), systems under mixed attacks will make the implementation of the optimal state estimation infeasible. We first get the optimal estimator for CPSs under mixed cyber-attacks. The optimal estimator consists of an exponentially growing number of components, and thus its computation effort exponentially grows in time [36][37][38].A mixed DDoS attack means an attack scenario in which more than one type of DDoS attack is used in combination (simultaneously or overlapping) against a target. The attacker may combine: High-rate flooding attacks (e.g. UDP flood, TCP SYN flood, DNS amplification) Low-rate / stealthy attacks (e.g. pulsing, low-rate flows intended to evade thresholds), Spoofed traffic (fake source IPs) Different protocols (TCP, UDP, ICMP) possibly reflection/amplification components [39].

Adaptive evasion (e.g. using ML-aware behaviours), Novel vectors (e.g. new protocols, SDN, edge, or cloud APIs), and Complex coordination (e.g. multi-phase or pulsing attacks) [40].

1. Bandwidth Depletion

It can be further classified into following attacks. Volume based attack, Amplification Attack, Flood Attack

Volume-based Attacks

These attacks aim to overwhelm the network bandwidth of the target. High volume of data and traffic is flooded to exhaust the bandwidth with not a specific target. Such type of attacks targets network infrastructure like router, firewall bandwidth etc. [41][42]. Volume based attacks can be of UDP flood, ICMP flood and DNS amplificationtype.

In UDP flood, attackers send a high volume of User Datagram Protocol (UDP) packets typically targeting random ports. Thus the attacked resources get overburdened and do not respond when required. It is a connectionless protocol. UDP packets are sent without establishing a connection between the sender and receiver. The attacker, or botnet of infected machines, sends UDP packets to random ports on the target server or device. These packets don't contain any useful information or requests, making them unnecessary for the target [43][44].

Whereas in ICMP flood, aattackers overloads the target with ICMP Echo Request (ping) packets. The target struggles to handle the incoming load which slows the services. The high volume of is attack is carried out for long duration to increase the intensity of attack. The attacker sends a large number of ICMP Echo Request packets (often referred to as "pings") to the target machine. The ICMP request is the type of packet used when someone runs the ping command to test if a machine is reachable over the network[45][46][47].

A particularly potent volumetric attack, DNS amplification, exploits vulnerabilities in the Domain name System servers. A small request is initiated to get relatively big response which further is forwarded towards the target to increase the magnitude of the traffic [48]49].

Amplification Attack

Another type of attack is aamplification attack, where attackers target certain vulnerabilities in web application often using botnets to make multiple requests that exploits familiar problems in services like apache and word press. [50][51].

DNS Amplification

DNS amplification uses DNS servers to amplify the attack by sending a small query that results in a large response.DNS amplification attacks massively exploit open recursive DNS servers mainly for performing bandwidth consumption DDoS attacks [52].The amplification effect lies in the fact that DNS response messages may be substantially larger than DNS query messages [53].

NTP Amplification

NTP amplification attacks exploits Network Time Protocol (NTP) servers to send a large amount of data to the victim. From 2013 - 2015 NTP DDoS attack growth significantly, the impact of DDoS resulted in losses and unavailability service of system [54].

SSDP

SSDP is part of the Universal Plug and Play protocol suite. It’s used for discovery of network devices like printers, smart TVs, routers, etc. It works over UDP port. This is a type of UDP-based amplification attack. An attacker sends spoofed SSDP requests (with the victim's IP as the source) to many SSDP-enabled devices. These devices then respond with much larger responses to the victim's IP. The result: the victim is flooded with massive traffic, causing denial of service [55].

Memcached

It is a high-performance memory caching system commonly used to reduce database load and accelerate dynamic web apps. The danger arises because UDP support: Memcached can listen on UDP (default port 11211).Lack of authentication / no access control: Many deployments expose Memcached to the public Internet (often erroneously).Large response payloads: A small “get” query can elicit very large responses (depending on size of cached objects).High amplification factor possible:

Attackers can exploit stored large items (or force large responses) to maximize amplification [56].

Flood Attacks

A flood attack refers broadly to sending a very large volume of packets to overwhelm a target system or network. It can be UDP flood, ICMP flood, SYN flood, Generic packet flood [57].

2. Resource Depletion Based Attacks

These attacks can be further classified into the following types of attack protocol attack. Malformed attack and Application layer attacks

Protocol attacks

These attacks target protocols to exhaust server resources or network equipment as it attacks the network layer. It targets the web server, local balancer or a firewall.Protocol attacks exploit the inherent weaknesses in the protocols themselves. These attacks are designed to consume server and network resources (such as CPU, memory, or bandwidth) or to cause disruptions in the communication channels [58][59].

When aattackers send a large number of SYN (synchronise) requests with a fake or incomplete source address, it is called SYN flood protocol attack. The server allocates resources in anticipation of completing the handshake, but the connection never finalises, leading to resource exhaustion. [60][61].To establish a connection, the TCP protocol uses a 3-step process known as the SYN-ACK handshake. The client sends a SYN (synchronize) packet to the server and it replies with a SYN-ACK (synchronize-acknowledge) packet. The client acknowledges by sending an ACK (acknowledge) packet to complete the handshake [62][63][64].

In another type of protocol attack called the Ping of Death attack, the attacker sends malformed ICMP Echo Request packets (ping requests) that are larger than the maximum allowed packet size (typically 65,535 bytes for IPv4)[65].

Malformed attack

The data to here must be divided into packets and encapsulated through seven layers from OSI protocol, from the upper application layer to the data link layer. When forging packets, attackers can launch DDoS attacks towards Software Defined Network controllers by making the data link matched by the Open Flow-enabled switch and be sent to the SDN controller, thus causing DDoS attacks towards SDN controller.[66][67][68].

A Malformed attack includes sending protocol messages that are not sent as per syntax or semantic rules—but are still accepted (or partially parsed) by the target—forcing costly error handling, state corruption, or crashes[69].

A SIP Message attack more refers to misuse of SIP protocol messages (INVITE, REGISTER, CANCEL etc.) possibly with malformed fields or flooding, to overload or crash VoIP infrastructures, research on VoIP-aware detection based on SIP behaviour[70][71].

AnIP Fragment attack disrupts IP packet fragmentation—sending a large number of small overlapping fragments or fragments out of order—to overwhelm the reassembly logic or manage normal detection; A Zero Payload DDos attack (or null-payload attack) sends IP, TCP, or other packets with no upper-layer payload (empty data), sometimes with abnormal headers, to resource waste or initiate implementation bugs; detection using "zero-payload packets" has been explored in work [72][73].

Application layer attacks

These are aimed at specific applications or services, often requiring less bandwidth but are harder to detect. As they copy authentic user behaviour so the actual user often goes unnoticed until the target is overwhelmed. GET Flood is most common type of application layer attack, where the attacker sends multiple GET requests to the server, requesting resources like HTML pages, images, or scripts. Requests appear like normal browsing requests, but the sheer volume of GET requests forces the server to use resources to process each one, such as retrieving files and handling data from the backend systems.[74][75]. Attacks even more damaging than GET floods, are POST flood attacks, where the attacker sends POST requests with large amounts of data (like form submissions) to the server. These requests often require additional server-side processing compared to GET requests, as the server needs to validate and process the data.Theyare often result in database queries, authentication, or other complex server-side operations that consume more resources [76][77].

3. Mixed Attacks /Advanced Emerging Attacks

Botnet –Based Attacks

A botnet is a network of zombie computers that have been designed to accept commands without the owner's knowledge [78]. Notably, the critical challenges against effective DDoS defense mechanisms are twofold: (i) To initiate DDoS flooding attacks, a large number of Zombies are used, and (ii) Zombies IP addresses are usually faked under the attacker's control. Thus, the attackers can possibly add more attack machines dwindles the clients' ability to purchase more incoming bandwidth, eventually crashing a website completely over time .An attacker (Master) controls a group of zombies, forming a botnet. Thus, botnets consist of masters, handlers, and agents (bots) whereby the master communicates to the bots through the handlers [79][80][81].

Hybrid attack

In the context of Distributed Denial of Service (DDoS),Hybrid attack refers to a type of attack that combines multiple DDoS attack techniques or strategies in a coordinated manner to amplify the impact on the targeted system. These attacks often combine different types of attacks, making detection and mitigation difficult [82][83].

SYN+ACK Floods with HTTP Flood sare type of hybrid attack targets both the network layer and application layer, overwhelming the target with a combination of SYN floods to exhaust server resources and HTTP flood .It attacks to choke application services.Sometimes the attacker initiates an HTTP connection to the target server by sending a partial HTTP request. This request is not complete and is deliberately malformed to keep the connection open indefinitely. This type of application layer is called HTTP flood [84][85].

Iot based attack

IoT-based attacks refer to cyber-attacks that specifically target the Internet of Things (IoT) devices and networks. IoT devices are everyday objects connected to the internet, such as smart thermostats, cameras, refrigerators, wearable health devices, industrial sensors, and home assistants [86][87].

Machine learning Based attack

Machine learning based attack refer to cyber-attacks on machine learning (ML) algorithms to identify susceptible devices, automate the attack process, and optimize the effectiveness of malicious actions. These attacks harness the power of machine learning to enhance the sophistication, speed and accuracy of cyber-attacks. As machine learning continues to evolve, attackers are increasingly using it to exploit systems in ways that are more dynamic, adaptive, and difficult to detect[88][89].

Reflective Attacks

Reflective attacks involve sending requests to an intermediary server, which then sends responses to the target.Different types of reflective attacks areDNS Reflection and CLDAP reflection attacks[90].DNS Reflection uses. DNS servers to reflect traffic to the victim. These amplification attacks are the most popular attacks in the Internet which require robust hardware and software for security assurance. Whereas, CLDAP reflection utilizes the Connection-less Lightweight Directory Access Protocol (CLDAP) to flood the victim with responses. DDoS attacks using the CLDAP protocol are increasing. CLDAP is an open-standard application that allows access to and maintenance of a wide range of network directory information. DDoS attacks using the CLDAP protocol exploit this, and can significantly increase the packet amplification rate as compared to existing UDP flooding attacks; this can immediately disable small and medium sized servers [91][92][93].

Table 1. Summary of Different Categories of Ddos Attacks with their Characteristic Features

Category of attack	Attack mechanism	Authors/reference papers cited	Objectives of attack	Target during attack
Bandwidth attack	Volume based attack	Argyraki, Katerina, and David R. Cheriton[41]. Mallick, Md Abu Imran, and Rishab Nath[42].	Attack on Network infrastructure including router, firewall, bandwidth	High volume of data and traffic is affected as overwhelm target attack
Bandwidth attack	Amplification attack	Hoque, Nazrul, Dhruba K. Bhattacharyya, and Jugal K. Kalita[50]. Aslan, Ömer, et al[51].	Disrupt the target services by consuming bandwidth and processing power	High volume of data is amplified and disrupted.
Bandwidth attack	Flood attack	Kumarasamy, Saravanan, andA. Gowrishankar[57].	Saturate bandwidth by consuming packet-processing capacity and deplete stateful resources	Target are Web servers, application servers , Load balancers, reverse proxies and firewalls
Resource depletion attack	Protocol attack	Abliz, Mehmud[58]. Douligeris, Christos, and Aikaterini Mitrokotsa[59]. Bogdanoski, Mitko, Tomislav Suminoski, and Aleksandar Risteski[60]. Eddy, Wesley. "Defenses against TCP SYN flooding attacks" [61].	Exploit weakness in network Device such as local balancer ,firewall	Targets network protocol service. and affects server
Resource depletion attack	Malformed attack	.Geneiatakis, Dimitris, et al.[69] Del Casale, Antonio, et al.[70] Feng, Xuewei, et al. "PMTUD is not Panacea[71]	Exhausts memory and state tables and trigger behaviour changes	Crashes CPU/memory, connection-table depletion, and detection evasion

Resource depletion attack	Application layer attack	. Cherinka, Brian, et al. "Marvin[74]. Nygren, Erik, Ramesh K. Sitaraman, and Jennifer Sun[75]. Li, Xiaowei, and Yuan Xue[76] Hacigumus, Hakan, Bala Iyer, and Sharad Mehrotra[77].	Exhaust various sessions and to consume backend resources	The attacks targets web servers, API and database and exploits specific applications.
Mixed attacks	Botnet-Based Attacks	Cooke, Evan, Farnam Jahanian, and Danny McPherson[78]. Hachem, Nabil, et al. "Botnets: lifecycle and taxonomy." [79]. Koroniotis, Nickolaos, Nour Moustafa, and Elena Sitnikova[80]. Li, Zhen, Qi Liao, and Aaron Striegel[81].	To deny access by saturating bandwidth, exhausting connections or CPU/memory on target	Botnet based attacks can target almost any online asset. Overwhelm defence via multiple vectors. It targets application, transport and network layers of the victim.
Mixed attacks	Hybrid attack	Bawany, Narmeen Zakaria, Jawwad A. Shamsi, and Khaled Salah[82]. Xing, Kai, et al. "Attacks and countermeasures in sensor networks: a survey[83]. Singh, Karanpreet, Paramvir Singh, and Krishan Kumar[84]. Vissers, Thomas, et al. "DDoS defense system for web services in a cloud environment[85].	Combine multi attack vector to increase the intensity of attack	Multilayers attacks are launched on target infrastructure
Advanced emerging attacks	Iot based attack	.Tsiknas, Konstantinos, et al. "Cyber threats to industrial IoT[86]. Siddique, Waqas Ahmed, Awais Khan Jumani, and Asif Ali Laghari[87].	Exploit weak, unpatched firmware, and lateral propagation to form botnets.	Target constrained devices and their ecosystems—smart cameras, routers, gateways, default-credential services, firmware update mechanisms, and cloud backends.

Advanced emerging attack	Machine learning Based attack	Corona, Igino, Giorgio Giacinto, and Fabio Roli.[88]. Cho, Jin-Hee, et al. "Toward proactive, adaptive defense[89].	Overwhelms training pipelines, targeting model inference and detection thresholds, and abusing autoencoders or classifiers to generate malicious traffic that is combined with benign flows.	Targets evasion of anomaly detectors, exploiting feature extractors.
Advanced emerging attack	Reflective Attacks	Mudgerikar, Anand, and Elisa Bertino [90]. Pakmehr, Amir, etal. "[91]. Salim, Mikail Mohammed, Shailendra Rathore, and Jong Hyuk Park [92]. Wang, Jincheng, et al. "Modern DDoS Threats and Countermeasures [93].	Hides the origin of attack And making filtering data difficult	Attackers spoof victim IP in requests to services like DNS, NTP or SNMP

Results & Discussion

From the past decade DDoS attacks have evolved in volume, complexity, and techniques posing challenges to the security and availability of online services. This research categorizes DDoS attacks into several primary types: bandwidth attacks, resource depletion attacks and mixed attacks and advanced ddos attacks. The increasing reliance on internet-based services has made Distributed Denial of Service (DDoS) attacks one of the most persistent and evolving threats in the cyber security landscape. This study categorizes DDoS attacks into four primary types—**bandwidth attacks**, **resource depletion attacks**, **mixed attacks**, and **advanced emerging attacks**—to better understand their characteristics, impact, and implications for defence mechanisms. Understanding the basic difference between different categories of DDoS attacks is crucial for developing layered and adaptive defence strategies.

Conclusion &Future scope

Through this paper an analysis is being conducted to understand how different types of DDos attacks hinder the smooth working of internet and the devices connected to it. Having a deep knowledge of types of attacks can help researchers to find better ways to handle these attacks and secure connections from Denial of Services hoax. By this paper we have tried to study the categories of different DDOS attacks so as to find different preventive measures as per the frequency and type of attack. While traditional bandwidth and resource depletion attacks continue to pose significant threats, the rise of mixed and advanced attacks demands more intelligent, context-aware, and automated mitigation solutions. The findings suggest that a one-size-fits-all approach is no longer viable.

References

1. Bahashwan, A.A.; Anbar, M.; Abdullah, N. New architecture design of cloud computing using software defined networking and network function virtualization technology. In Advances in Intelligent Systems and Computing; Springer: Cham, Switzerland, 2020; Volume 1073, pp. 705–713.
2. Al-Dhuraibi, Yahya, et al. "Elasticity in cloud computing: state of the art and research challenges." IEEE Transactions on services computing 11.2 (2017): 430-447
3. Islam, Rafia, et al. "The future of cloud computing: benefits and challenges." International Journal of Communications, Network and System Sciences 16.4 (2023): 53-65.
4. Alashhab, Z.R.; Anbar, M.; Singh, M.M.; Leau, Y.B.; Al-Sai, Z.A.; Abu Alhayja'a, S. Impact of coronavirus pandemic crisis on technologies and cloud computing applications. J. Electron. Sci. Technol. **2021**, 19, 100059.
5. M. Alduailij, Q.W. Khan, M. Tahir, M. Sardaraz, F. Malik.Machine learning based ddos attack detection using mutual information and random forest feature importance method Symmetry (Basel), 14 (6) (2022), p. 1095.
6. Marston, Sean, et al. "Cloud computing—The business perspective." Decision support systems 51.1 (2011): 176-189.
7. Heng, Stefan, et al. "Cloud computing." Freundliche Aussichten für die Wolke, Deutsche Bank DB Research, Economics. Digitale Ökonomie und struktureller Wandel, Frankfurt am Main (2012).
8. Wyld, David C. Moving to the cloud: An introduction to cloud computing in government. IBM Center for the Business of Government, 2009.
9. Tabrizchi, Hamed, and Marjan Kuchaki Rafsanjani. "A survey on security challenges in cloud computing: issues, threats, and solutions." The journal of supercomputing 76.12 (2020): 9493-9532.
10. Yan, Qiao, et al. "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges." IEEE communications surveys & tutorials 18.1 (2015): 602-622.
11. Bawany, Narmeen Zakaria, Jawwad A. Shamsi, and Khaled Salah. "DDoS attack detection and mitigation using SDN: methods, practices, and solutions." Arabian Journal for Science and Engineering 42.2 (2017): 425-441.
12. Praseed, Amit, and P. Santhi Thilagam. "DDoS attacks at the application layer: Challenges and research perspectives for safeguarding web applications." IEEE Communications Surveys & Tutorials 21.1 (2018): 661-685.
13. Rossow, Christian. "Amplification Hell: Revisiting Network Protocols for DDoS Abuse." NDSS. 2014.

14. Gupta, Brij B., and Omkar P. Badve. "Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment." Neural Computing and Applications 28.12 (2017): 3655-3682.
15. Shaar, Fadi, and Ahmet Efe. "DDoS attacks and impacts on various cloud computing components." International Journal of Information Security Science 7.1 (2018): 26-48.
16. Lohachab, Ankur, and Bidhan Karambir. "Critical analysis of DDoS—An emerging security threat over IoT networks." Journal of Communications and Information Networks 3.3 (2018): 57-78.
17. Vahdani Amoli, Payam. "Unsupervised network intrusion detection systems for zero-day fast-spreading network attacks and botnets." Jyväskylä studies in computing 231 (2015).
18. Musa, Nura Shifa, et al. "machine learning and deep learning techniques for distributed denial of service anomaly detection in software defined networks—current research solutions." IEEE Access 12 (2024): 17982-18011.
19. Ali, Tariq Emad, Yung-Wey Chong, and Selvakumar Manickam. "Machine learning techniques to detect a DDoS attack in SDN: A systematic review." Applied Sciences 13.5 (2023): 3183.
20. Farsimadan, Eslam. "A Study of some ML and DL-based Strategies for Network Security." (2023).
21. Alazab, Mamoun, et al. "Deep learning for cyber security applications: A comprehensive survey." Authorea Preprints (2023).
22. Dasgupta, Dipankar, Zahid Akhtar, and Sajib Sen. "Machine learning in cybersecurity: a comprehensive survey." The Journal of DefenseModeling and Simulation 19.1 (2022): 57-106.
23. Sarker, Iqbal H. "Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective." SN Computer Science 2.3 (2021): 154.
24. Qureshi, Sirajuddin, et al. "A hybrid DL-based detection mechanism for cyber threats in secure networks." Ieee Access 9 (2021): 73938-73947.
25. Wu, Yirui, Dabao Wei, and Jun Feng. "Network attacks detection methods based on deep learning techniques: A survey." Security and Communication Networks 2020.1 (2020): 8872923.
26. Douligeris, Christos, and Aikaterini Mitrokotsa. "DDoS attacks and defense mechanisms: classification and state-of-the-art." Computer networks 44.5 (2004): 643-666.
27. Bhattacharyya, Dhruba Kumar, and Jugal Kumar Kalita. DDoS attacks: evolution, detection, prevention, reaction, and tolerance. CRC Press, 2016.
28. Al-Abassi, Abdulrahman, Jacob Sakhnini, and Hadis Karimipour. "Unsupervised stacked autoencoders for anomaly detection on smart cyber-physical grids." 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC). IEEE, 2020.

29. Tufail, Shahid, et al. "A hybrid machine learning-based framework for data injection attack detection in smart grids using PCA and stacked autoencoders." IEEE Access (2025).
30. Vinayakumar, R., K. P. Soman, and Prabaharan Poornachandran. "Evaluating deep learning approaches to characterize and classify malicious URL's." Journal of Intelligent & Fuzzy Systems 34.3 (2018): 1333-1343.
31. Tian, Zhihong, et al. "A distributed deep learning system for web attack detection on edge devices." IEEE Transactions on Industrial Informatics 16.3 (2019): 1963-1971.
32. Potluri, Srinivas. "A Deep Learning-Driven Framework for Detecting Anomalous Data Breaches in Distributed Cloud Storage Infrastructures." International Journal of Artificial Intelligence, Data Science, and Machine Learning 5.3 (2024): 80-87.
33. Butt, Umer Ahmed, et al. "A review of machine learning algorithms for cloud computing security." Electronics 9.9 (2020): 1379.
34. Hill, W., Acquaah, Y.T., Mason, J. et al. DDoS in SDN: a review of open datasets, attack vectors and mitigation strategies. Discov Appl Sci 6, 472 (2024).
35. Hubballi, N., Barsha, N.K. (2024). Mitigating Resource Depletion and Message Sequencing Attacks in SCADA Systems. In: Barolli, L. (eds) Advanced Information Networking and Applications. AINA 2024. Lecture Notes on Data Engineering and Communications Technologies, vol 201. Springer, Cham.
36. Ao, Wei, Yongduan Song, and Changyun Wen. "Distributed secure state estimation and control for CPSs under sensor attacks." IEEE transactions on cybernetics 50.1 (2018): 259-269.
37. Olowononi, Felix O., Danda B. Rawat, and Chunmei Liu. "Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for CPS." IEEE Communications Surveys & Tutorials 23.1 (2020): 524-552.
38. Yohanandhan, Rajaa Vikhram, et al. "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications." IEEE Access 8 (2020): 151019-151064.
39. Zhou, L., Zhu, Y., Xiang, Y. et al. A novel feature-based framework enabling multi-type DDoS attacks detection. World Wide Web **26**, 163–185 (2023).
40. Zargar, Saman Taghavi, James Joshi, and David Tipper. "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." IEEE communications surveys & tutorials 15.4 (2013): 2046-2069.
41. Argyraki, Katerina, and David R. Cheriton. "Scalable network-layer defense against internet bandwidth-flooding attacks." IEEE/ACM Transactions on networking 17.4 (2009): 1284-1297.
42. Mallick, Md Abu Imran, and Rishab Nath. "Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments." World Scientific News 190.1 (2024): 1-69.

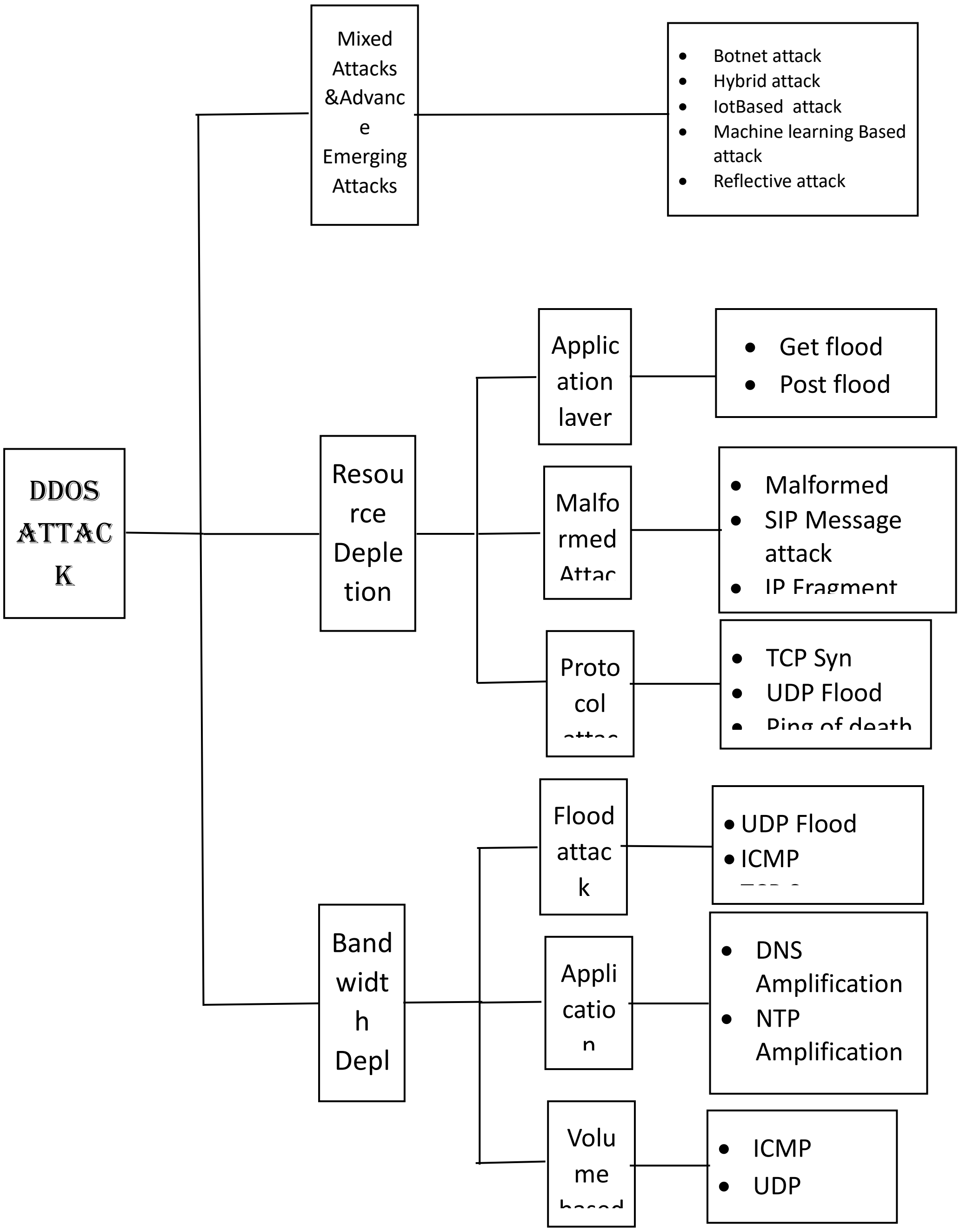
43. Thomas, Daniel R., Richard Clayton, and Alastair R. Beresford. "1000 days of UDP amplification DDoS attacks." 2017 APWG Symposium on Electronic Crime Research (eCrime). IEEE, 2017.
44. Huraj, Ladislav, Marek Simon, and Tibor Horák. "IoT measuring of UDP-based distributed reflective DoS attack." 2018 IEEE 16th international symposium on intelligent systems and informatics (SISY). IEEE, 2018.
45. Hunt, Craig. TCP/IP network administration. Vol. 2. " O'Reilly Media, Inc.", 2002.
46. Bellovin, Steven M. "Packets found on an internet." ACM SIGCOMM Computer Communication Review 23.3 (1993): 26-31.
47. Chapman, D. Brent. "Network (In) Security Through IP Packet Filtering." USENIX Summer. Vol. 21. 1992.
48. Anagnostopoulos, Marios, et al. "DNS amplification attack revisited." Computers & Security 39 (2013): 475-485.
49. Nawrocki, Marcin, et al. "The far side of DNS amplification: tracing the DDoS attack ecosystem from the internet core." Proceedings of the 21st ACM Internet Measurement Conference. 2021.
50. Hoque, Nazrul, Dhruba K. Bhattacharyya, and Jugal K. Kalita. "Botnet in DDoS attacks: trends and challenges." IEEE Communications Surveys & Tutorials 17.4 (2015): 2242-2270.
51. Aslan, Ömer, et al. "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions." Electronics 12.6 (2023): 1333.
52. Anagnostopoulos, Marios, et al. "DNS amplification attack revisited." Computers & Security 39 (2013): 475-485.
53. Yazdani, Ramin, et al. "A matter of degree: characterizing the amplification power of open DNS resolvers." International Conference on Passive and Active Network Measurement. Cham: Springer International Publishing, 2022.
54. Shukla, Praveen, C. Rama Krishna, and Nilesh Vishwasrao Patil. "Iot traffic-based DDoS attacks detection mechanisms: A comprehensive review." Journal of Supercomputing 80.7 (2024).
55. Liu, X. et al. (2019). A Multi-location Defence Scheme Against SSDP Reflection Attacks in the Internet of Things. In: Ning, H. (eds) Cyberspace Data and Intelligence, and Cyber-Living, Syndrome, and Health. CyberDICyberLife 2019 2019. Communications in Computer and Information Science, vol 1137. Springer, Singapore.
56. Singh, Kulvinder, and Ajit Singh. "Memcached DDoS exploits: Operations, vulnerabilities, preventions and mitigations." 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS). IEEE, 2018.
57. Kumarasamy, Saravanan, and A. Gowrishankar. "An active defense mechanism for TCP SYN flooding attacks." arXiv preprint arXiv:1201.2103 (2012).
58. Abliz, Mehmud. "Internet denial of service attacks and defense mechanisms." University of Pittsburgh, Department of Computer Science, Technical Report (2011): 1-50.

59. Douligeris, Christos, and Aikaterini Mitrokotsa. "DDoS attacks and defense mechanisms: classification and state-of-the-art." Computer networks 44.5 (2004): 643-666.
60. Bogdanoski, Mitko, Tomislav Suminoski, and Aleksandar Risteski. "Analysis of the SYN flood DoS attack." International Journal of Computer Network and Information Security (IJCNIS) 5.8 (2013): 1-11.
61. Eddy, Wesley. "Defenses against TCP SYN flooding attacks." Cisco Internet Protocol Journal (2006).
62. Kepçeoğlu, Buğra, Azhar Murzaeva, and Sercan Demirci. "Performing energy consuming attacks on iot devices." 2019 27th Telecommunications Forum (TELFOR). IEEE, 2019.
63. Douligeris, Christos, and Aikaterini Mitrokotsa. "DDoS attacks and defense mechanisms: classification and state-of-the-art." Computer networks 44.5 (2004): 643-666.
64. Convery, Sean, and Darrin Miller. "Ipv6 and ipv4 threat comparison and best-practice evaluation (v1. 0)." Presentation at the 17th NANOG 24 (2004): 16.
65. Abdollahi, Asrin, and Mohammad Fathi. "An intrusion detection system on ping of death attacks in IoT networks." Wireless Personal Communications 112.4 (2020): 2057-2070.
66. Yan, Qiao, Qingxiang Gong, and Fang-an Deng. & quot; Detection of DDoS attacks against wireless SDNcontrollers based on the fuzzy synthetic evaluation decision-making model.&quot; Adhoc & amp; Sensor Wireless Networks 33 (2016).
67. Deshmukh, Rashmi V., and Kailas K. Devadkar. & quot; Understanding DDoS attack &amp; its effect in cloud environment. &quot; Procedia Computer Science 49 (2015): 202-210.
68. Sonar, Krushang, and Hardik Upadhyay. & quot; A survey: DDOS attack on Internet of Things.&quot; International Journal of Engineering Research and Development 10.11 (2014): 58-63.
69. Geneiatakis, Dimitris, et al. "A framework for protecting a SIP-based infrastructure against malformed message attacks." Computer Networks 51.10 (2007): 2580-2593.
70. Del Casale, Antonio, et al. "Psychosis risk syndrome comorbid with panic attack disorder in a cannabis-abusing patient affected by Arnold–Chiari malformation type I." General Hospital Psychiatry 34.6 (2012): 702-e5.
71. Feng, Xuewei, et al. "PMTUD is not Panacea: Revisiting IP Fragmentation Attacks against TCP." NDSS. 2022.
72. He, Zhitao, and Thiemo Voigt. "Droplet: A new denial-of-service attack on low power wireless sensor networks." 2013 IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems. IEEE, 2013.
73. Dimolianis, Marinos, Adam Pavlidis, and Vasilis Maglaris. "Signature-based traffic classification and mitigation for DDoS attacks using programmable network data planes." IEEE Access 9 (2021): 113061-113076.

74. Cherinka, Brian, et al. "Marvin: A tool kit for streamlined access and visualization of the SDSS-IV MaNGA data set." The Astronomical Journal 158.2 (2019): 74.
75. Nygren, Erik, Ramesh K. Sitaraman, and Jennifer Sun. "The akamai network: a platform for high-performance internet applications." ACM SIGOPS Operating Systems Review 44.3 (2010): 2-19.
76. Li, Xiaowei, and Yuan Xue. "A survey on server-side approaches to securing web applications." ACM Computing Surveys (CSUR) 46.4 (2014): 1-29.
77. Hacigumus, Hakan, Bala Iyer, and Sharad Mehrotra. "Providing database as a service." Proceedings 18th International Conference on Data Engineering. IEEE, 2002.
78. Cooke, Evan, Farnam Jahanian, and Danny McPherson. "The zombie roundup: Understanding, detecting, and disrupting botnets." SRUTI 5 (2005): 6-6.
79. Hachem, Nabil, et al. "Botnets: lifecycle and taxonomy." 2011 Conference on Network and Information Systems Security. IEEE, 2011.
80. Koroniotis, Nickolaos, Nour Moustafa, and Elena Sitnikova. "Forensics and deep learning mechanisms for botnets in internet of things: A survey of challenges and solutions." IEEE Access 7 (2019): 61764-61785.
81. Li, Zhen, Qi Liao, and Aaron Striegel. "Botnet economics: uncertainty matters." Managing information risk and the economics of security. Boston, MA: Springer US, 2008. 245-267.
82. Bawany, Narmeen Zakaria, Jawwad A. Shamsi, and Khaled Salah. "DDoS attack detection and mitigation using SDN: methods, practices, and solutions." Arabian Journal for Science and Engineering 42.2 (2017): 425-441.
83. Xing, Kai, et al. "Attacks and countermeasures in sensor networks: a survey." Network security. Boston, MA: Springer US, 2010. 251-272.
84. Singh, Karanpreet, Paramvir Singh, and Krishan Kumar. "Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges." Computers & security 65 (2017): 344-372.
85. Vissers, Thomas, et al. "DDoS defense system for web services in a cloud environment." Future Generation Computer Systems 37 (2014): 37-45.
86. Tsiknas, Konstantinos, et al. "Cyber threats to industrial IoT: a survey on attacks and countermeasures." IoT 2.1 (2021): 163-186.
87. Siddique, Waqas Ahmed, Awais Khan Jumani, and Asif Ali Laghari. "Introduction to internet of things with flavor of blockchain technology." Blockchain. Chapman and Hall/CRC, 2022. 51-72.
88. Corona, Igino, Giorgio Giacinto, and Fabio Roli. "Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues." Information sciences 239 (2013): 201-225.
89. Cho, Jin-Hee, et al. "Toward proactive, adaptive defense: A survey on moving target defense." IEEE Communications Surveys & Tutorials 22.1 (2020): 709-745.
90. Mudgerikar, Anand, and Elisa Bertino. "Iot attacks and malware." Cyber Security Meets Machine Learning. Singapore: Springer Singapore, 2021. 1-25.

91. Pakmehr, Amir, et al. "DDoS attack detection techniques in IoT networks: a survey." Cluster Computing 27.10 (2024): 14637-14668.
92. Salim, Mikail Mohammed, Shailendra Rathore, and Jong Hyuk Park. "Distributed denial of service attacks and its defenses in IoT: A survey." Journal of Supercomputing 76.7 (2020).
93. Wang, Jincheng, et al. "Modern DDoS Threats and Countermeasures: Insights into Emerging Attacks and Detection Strategies." arXiv preprint arXiv:2502.19996 (2025)

Figure 1: Different types DDoS Attacks


DDOS ATTAC K
Mixed Attacks &Advanc e Emerging Attacks
Botnet attack
Hybrid attack
IotBased attack
Machine learning Based attack
Reflective attack
Resou rce Deple tion
Applic ation laver
Get flood
Post flood
Malfo rmed Attac
Malformed
SIP Message attack
IP Fragment
Proto col attac
TCP Syn
UDP Flood
Ping of death
Band widt h Depl
Flood attac k
UDP Flood
ICMP
Appli catio n
DNS Amplification
NTP Amplification
Volu me based
ICMP
UDP