Contents lists available at ScienceDirect

Computers & Security

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

A comprehensive study of DDoS attacks over IoT network and their countermeasures

Pooja Kumari*, Ankit Kumar Jain

Computer Engineering Department, National Institute of Technology, Kurukshetra, India

ARTICLE INFO

Article history:
Received 4 January 2022
Revised 4 January 2023
Accepted 8 January 2023
Available online 13 January 2023

Keywords:
Internet of things
DDoS attack
Botnet
Machine learning
Software defined network

ABSTRACT

IoT offers capabilities to gather information from digital devices, infer from their results, and maintain and optimize these devices in different domains. IoT is heterogeneous in nature, which makes it prone to various security threats like confidentiality and integrity breaches, lack of availability of resources, trust issues, etc. The security concerns lead to different attacks over the system, and the Distributed Denial of Services (DDoS) bout is growing generously. DDoS is an assault that targets the availability of resources and servers of a network by flooding the communication medium from distinct locations by utilizing various IoT devices, which makes it harder to detect. Thus, analyzing and defending DDoS is a protruding field of research these days. The paper gives a thorough knowledge of DDoS over IoT. In this, we have critically analysed the existing DDoS variants, IoT Security issues, the execution of DDoS attempts, along with the exploitation of IoT devices and creation of them in Botnets or zombies. Moreover, the paper will also cover prevailing DDoS defense methodologies as well as their comparative analysis for ease of understanding.

© 2023 Elsevier Ltd. All rights reserved.

1. Introduction

IoT has reached heights in recent years, the Internet of Things explicates the physical world as a vast network, which consists of those devices that have a digital identity. These devices may be too tiny and large as well such as sensors, actuators, mobile phones, televisions, light bulbs, thermostats, clinical gears, smartwatches, software, and so forth. To understand the concept of IoT a developing range of physical devices is associated with the internet at an exponential rate (Al-Fuqaha, 2015). Hence, the term IoT is stated as an assemblage of smart objects with the basic and premise goal of “Connecting the Unconnected”. In IoT, the embedded smart gadgets observe their current circumstance, execute common tasks, convey the message straightforwardly and synchronize the decision unconventionally without human mediation. Since IoT Provides excellent connectivity and easy communication, the number of organizations that have shifted towards this technology is increasing tremendously (Taylor, 2013). Nowadays, IoT has become a prominent network including a huge number of gadgets connecting to simplify human tasks (Gantz and Reinsel, 2012). According to the research, there are currently over 5 trillion gadgets that have access to the internet. The market returns for the technology surpassed $100 billion in 2017 ever in the era, and the global marketplace for IoT end node products reached 212 billion USD by the end of 2019. Now, predictions imply that by 2025, this amount will rise to approximately 1.6 trillion (Vailshery, 2021; Jia et al., 2020).

All these statistics, however, highlight a conceivably critical and high-speed development of the IoT. Conventional components manufacturing companies now have a unique chance to change their items into "smart objects" as a result of this evolution. To deliver Quality Service for a mix of Machine-to-Machine (M2M) (Farooq et al., 2015; Shafiq et al., 2012), Person-to-Machine (P2M), and Person-to-Person (P2P) traffic flows, Internet Service Providers (ISPs) must facilitate their networks, if the Internet of Things and related administrations are to be widely adopted (Al-Fuqaha, 2015; Atzori et al., 2010).

This ubiquitous growth of IoT applications makes the technology more vulnerable and prone to attacks (Gubbi et al., 2013). Although service domains of IoT are arising uninterruptedly yet the security concerns are hostile (Gantz and Reinsel, 2012). Since IoT works on assorted networks embedded with large as well as small devices. The small devices have low computational power and less storage capacity and hence protection mechanisms and the cryptographic algorithm used for security are hard to implement over them. As the small IoT devices do not have any privacy-preserving algorithms, aggressors exploit their vulnerabilities and use them as a bot to persuade the assault.

There are a lot of assaults that are performed over IoT networks and one of them is the Distributed Denial of Service (DDoS) attack.

* Corresponding author.
E-mail address: poojakumari.cse7@gmail.com (P. Kumari).

https://doi.org/10.1016/j.cose.2023.103096
0167-4048/© 2023 Elsevier Ltd. All rights reserved.

By definition, a DDoS attack upsets the network services and resources for the authorized users while requesting that. DDoS attack disturbs the network by flooding the server or site with multiple requests at the same time from different locations and which in turn reduces the genuine users' bandwidth (Lau et al., 2000). DDoS assault is quite problematic to detect as it uses distinct locations as well as various devices to perform the attack. In IoT, the assaulter uses the IoT gadgets as a bot to persuade the attack which makes it harder to detect and prevent. Because the bots an intruder uses are IoT legitimate devices and as they are low-powered devices with less storage do not provide any security and hence are easily attacked.

DDoS is the most common sort of network disruption assault and one of the most serious issues that IT consultants and security professionals face. Some of the major crashes due to DDoS are:

- One of the most infamous DDoS assaults in online attacks has happened in September 2016 using the Mirai Botnet (Jia et al., 2020). Mirai is a potential DDoS tool that is proficient in easily managing around 3 million IoT device bots (Prasad et al., 2019). The Mirai Botnet has brought down a few noticeable sites including Netflix, CNN, Twitter, Reddit, etc. by using 1.2 Tbps bandwidth strength (Jerkins, 2017). The tool infected over 1 million devices, which makes it the largest assault that happened in the year (Zare et al., 2017). This DDoS attack was recorded over Dyn's servers. Dyn operates the majority of the United States' DNS servers (McDermott et al., 2018).
- In 2018 GitHub confronted 1.35 Tbps of delayed traffic, resulting in a 10-minute outage. The site had the option of sending traffic to DDoS mitigation provider Akamai Prolexic's (Kotey et al., 2019) association to mitigate the ongoing DDoS crash (Singh et al., 2020; Pande and Khamparia, 2019).
- Amazon Web Services (AWS) was struck by a huge DDoS assault which was recorded in February 2020, with a volume of 2.3 Tbps. The attack on AWS was 44% larger than any other volumetric assault (Crane, 2020).
- In October 2020 Google uncovered interestingly that their foundation had "assimilated a 2.5 Tbps DDoS in September 2017, the perfection of a six-month campaign that used various techniques for the attack," which would retroactively make it larger than the aforementioned attacks (Kovacs, 2020; Devdiscourse, 2020).
- In September 2021 Yandex (a Russian Internet Giant) faced a massive DDoS attempt with 21.8 million RPS (Requests Per Second). The attack was recorded from 7th August 2021 (at 5.2 MRPS) to 5th September the year (Raza, 2021).

Fig. 1 depicts the statistical data of the biggest outbreaks that occurred due to DDoS attacks for respective previous years based on the attacking power (Frolova, 2021; Gutnikov et al., 2021). We can observe from the figure that these assaults as well as their intensity of them are increasing exponentially day by day.

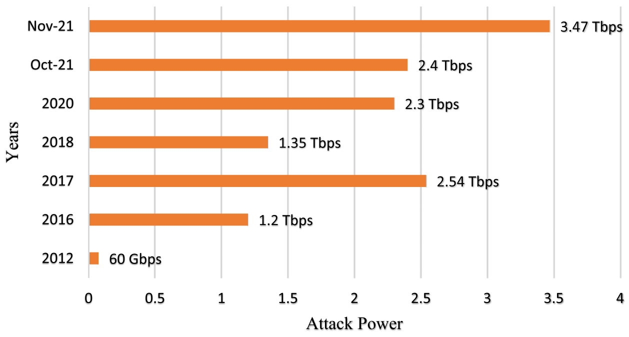

Fig. 1. Major DDoS Attacks Recorded in the previous years based on the Attack power.

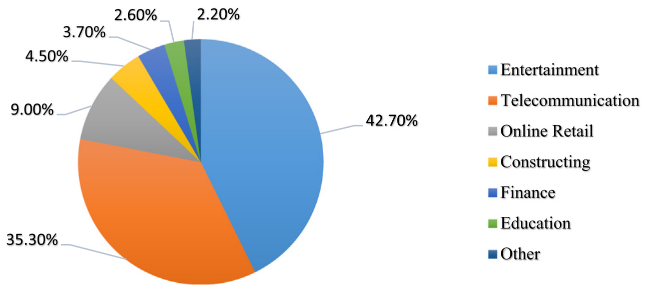

Fig. 2. Statistical Division of DDoS Attacks in 2021.

The statistics show the major outbreaks of the particular year. The attackers target distinct areas of the industry to persuade the attack at a high rate. In addition to these statistics, recently in the year 2021, the entertainment industry faced the highest rate of DDoS followed by the telecommunication field. Fig. 2 shows the statistical division of DDoS Attacks by industries in the year 2021 (Gutnikov et al., 2021). It shows how attackers target a specific field based on the popularity of that industry and the number of users using it.

There exists a similar situation to a DDoS attack termed "Flash Events" which floods the network resulting in a server crash. A flash event can be described as a situation when the server or the system ran out of resources (Behal and Kumar, 2017). The situation happens when a lot of users try to access a computer or a web service. The main difference between Flash Events and DDoS is that flash events are unintentional and caused by legitimate traffic while DDoS is performed intentionally by an attacker. Sometimes the attacker misuses this situation and launches an attack during the flash event. Some recent flash events are:

- WazirX is a crypto currency trading website in India and the 'WRX' crypto token grew by 200% from $1 billion to $1.23 billion which in turn caused a server outage for about an hour (Palepu, 2021) in April 2021.
- In July 2020 the CBSE website got crashed after the Central Board of Education uploaded the class 12 board results. The crash happened due to millions of students were trying to access the site at the same time (TV, 2020).
- In 2020 the Google server crashed for about 30 min due to a failure in the company's authentication tool. The outage affected the services like Gmail, Google Calendar, and YouTube (Hern, 2020).
- On 21st August 2016, an Australian Census website started responding untimely because millions of users were accessing that to fill in their details and the website got crashed due to insufficient services (Behal and Kumar, 2017).

Hence, it is noteworthy that the denial of service is growing rapidly and it can be performed intentionally for numerous benefits. Due to the different vulnerabilities of IoT devices and the enormous growth of DDoS variants, the security concern is a priority now, and to mitigate these issues several kinds of research and surveys have been carried out to find solutions to prevent the IoT devices and the network. Some of them are discussed and compared in the related work section.

The rest of the paper is further systematized into distinct segments such that Section 2 discusses the literature and related articles for DDoS to get a thorough knowledge about the DDoS attack over IoT. The section provides what has been done in the previous years to this extent and how our survey is different from the previous ones. Section 3 renders the IoT security concerns, which are

Table 1
Comparison of Different Surveys on DDoS Attacks over IoT Network.

Research Work	Year	Security Challenges and Requirements of IoT Layers	Different Botnet Variants	DDoS Attack Architecture	Taxonomy of DDoS Attacks	Comparison among DDoS Defense Mechanisms	Preventive measures for DDoS
Mahjabin et al. (2017)	2017	No	No	No	Yes	No	Yes
Manavi (2018)	2018	No	No	No	No	Yes	No
Lohachab and Karambir (2018)	2018	No	No	No	Yes	Yes	No
Chen et al. (2018)	2018	Yes	No	No	Yes	No	No
Roohi et al. (2019)	2019	Yes	No	No	Yes	No	No
Munshi et al. (2020)	2020	No	Partially Covered	No	Yes	No	No
Irum et al. (2020)	2020	No	No	No	No	Yes	Yes
Salim et al. (2020)	2020	No	Partially Covered	No	Yes	Yes	Yes
Vishwakarma and Jain (2020)	2020	No	Partially Covered	No	Yes	Yes	No
Hadhrami and Hussain (2021)	2021	Yes	No	No	Yes	Yes	No
Our Survey	2022	Yes	Yes	Yes	Yes	Yes	Yes

faced by the users while using IoT gadgets, or IoT-incorporated networks followed by Taxonomy of Attacks, Security Issues, and Requirements of IoT Layers in segment 4 which focuses on the layers present in the IoT architecture. Section 5 discusses the motivation behind performing the attack, and why the attacker chooses IoT devices for attacking the network. The section presents some of the vital reasons why an intruder intends to launch an assault. Section 6 discusses DDoS in IoT, the diverse variants of DDoS attacks, the architecture of DDoS, and how a Botnet is created as well as various botnets. This section gives a detailed explanation of how the DDoS attack is performed over an IoT network by hacking IoT devices and making bots. Further, we have listed a few variants of botnets that are utilized by attackers, the DDoS architectural models, and different types of DDoS attacks. Further, Section 7 discusses various DDoS defense mechanisms and their comparative analysis followed by Sections 8 and 9 which refers to some preventive measures, open issues, and challenges, respectively. The last section, Section 10 concludes the paper's findings.

2. Related work

Many researchers have surveyed DDoS attacks and the majority of them have covered the DDoS assault over traditional networks. The researchers have explored the different types of DDoS attacks and the countermeasures to mitigate them in their work but, a few of them have gone more specific about the DDoS attack over the IoT network. Salim et al. (2020) have presented a detailed explanation of DDoS attacks over the IoT network which includes the types of DDoS attacks, the motivation behind them, and defense mechanisms to detect and prevent the network from the attacks. Along with these topics, the authors have also partially covered various botnets to execute the attack. McDermott et al. (2018) have provided a detection methodology using deep learning approaches which detect the assaults carried out by IoT botnets. Manavi (2018) provides a survey of defense mechanisms for DDoS assault covering the types of DDoS and countermeasures for them. However, the work does not cover the distinct IoT botnets, IoT vulnerabilities, and some others such as the motivation for conducting the assault. Thus, there are many surveys present in this area in which the researchers have anticipated different DDoS detection methodologies, prevention mechanisms, and defense techniques, and many of them have keenly analyzed and compared these. However, most of the surveys do not provide the different variants of DDoS, the evolving IoT botnets, and their countermeasures. Table 1 compares our survey with the other ones based on some parameters:

We have gone through these surveys to get a thorough knowledge of the research area and to cover enough content to understand the DDoS attack and its harmfulness for the IoT devices as well as the network. Moreover, Table 1 gives a comparative analysis of various surveys with ours based on certain parameters which are further discussed in the remaining sections of the paper.

3. Security challenges in IoT

Regardless of existing possibilities for reforming the present network paradigm, there are a few IoT security vulnerabilities that need to be investigated (Mahmoud et al., 2015). IoT delivers effective and efficient services to its end users, yet it faces some security and privacy challenges due to the devices' vulnerabilities and vast heterogeneous networks. Some of the security issues are listed here as shown in Fig. 3 (Alrawais et al., 2017):

3.1. Authentication

IoT network is comprised of digital devices. Some low-powered devices do not have enough storage as well as computational power to implement cryptographic algorithms for authentication purposes. This, in turn, makes these devices exploitable and

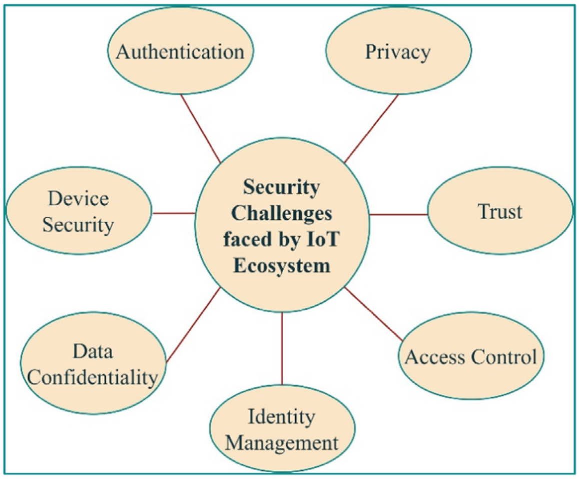

Fig. 3. Security Issues in IoT.

the network as well. The aggressor exploits these gadgets and sneaks into the network to get access (Pateriya and Sharma, 2011; Sonar and Upadhyay, 2014).

3.2. Trust

The IoT ecosystem works on a heterogeneous network having numerous devices, actuators, etc. for information gathering. This generates a trust issue among the devices and the users also and trust plays a vital role in preserving secure and reliable IoT services. To design a trust model, an IoT network should maintain integrity, confidentiality, availability, and authenticity (Akram et al., 2018; Noor and Hassan, 2019).

3.3. Privacy

The attacker exploits the vulnerabilities of IoT devices which leads to privacy leakage as in data leaks gathered by the sensors, location of the gadgets, passcodes to gain access, etc. The devices' vulnerabilities arise due to their resource-constrained nature (Atzori et al., 2010).

3.4. Access control

Access control ensures that only authentic users can access the information, devices, and network resources from the network environment. But IoT uses low-powered and lossy network devices with limited resources such as power and bandwidth, thus access control is a challenge for the IoT ecosystem; also access control is a task in itself for distributed data (Pateriya and Sharma, 2011).

3.5. Data confidentiality

IoT devices are increasing day by day resulting in the generation of massive data volume. But due to gadgets' limitations, this huge data is difficult to process at the perception level. Hence the gathering layer transfers it to the cloud at the decision unit or data processing layer which makes information confidentiality preservation a tricky task (Akram et al., 2018).

3.6. Identity management

The IoT ecosystem has countless interconnected devices and their management is quite difficult. Because dynamically assigning a unique id to all devices and maintaining them is a challenge. Identity management can be obtained by using the IPV6 architecture as it provides auto-configuration features (Gupta et al., 2009).

3.7. Device security

The Internet of Things (IoT) connects a large number of devices that communicate across networks. Despite any security precautions, the system provides minimal control because if any one of the devices is attacked, the security can be breached (Gupta et al., 2009).

These security issues and vulnerabilities attract a hacker to exploit them and use them for intrusion purposes. The attacker utilizes these security issues to persuade the attacks and to gain access to the network. The next section discusses different attacks performed over the IoT architectural layers and the security requirements to procure them.

4. Taxonomy of attacks, security issues, and requirements of IoT layers

This section provides a categorization of attacks and security challenges in each layer of IoT architecture. The implementation of different IoT applications in different areas and IoTs' functionality over the domain determines its architecture, even though, its framework is constructed on a basic procedural flow (Zhang and Qu, 2013). Based on these facts there are different IoT network architectures, the most commonly used and core IoT design is a contemplation of four successive layers namely: Application Layer, Middleware Layer, Network Layer, and the Perception Layer. These layers face distinct assaults to gain unauthorized access to the network. Table 2 shows IoT attacks faced by each layer, the main security challenges, and the basic requirements to mitigate these security and privacy concerns. These security concerns are the anomalies that occur due to loopholes present in the respective layer. The security requirements mentioned in the table can be implemented by using different defense mechanisms which are further discussed in Section 7 of the paper.

Table 2 lists different attacks that can be launched by the intruder due to the security issues at each layer. The layered IoT architecture consists of different layers with respective functionalities, such as the perception layer collects the raw data from the end devices and sends it to the upper layer, which is the network layer. Similarly, the network layer routes the data and transfers it to the middle layer for data processing, which is then further sent to the topmost layer. While performing these tasks the layers face some security loopholes and hacker exploits them to conduct the assault. Section 5 answers the question that what motivates the assaulter to conduct these attacks and why he/she opts for IoT devices for this purpose.

5. Motivations and targets of DDoS attack

DDoS attacks are progressively becoming the most common form of cyber threat, according to recent market research, and have risen increasingly in both number and volume in the past year. The trend is towards a shorter length of attack but a greater number of packet-by-second attacks. DDoS assaults can affect anyone, from a single home user to a country. A web-based corporate website, a business group, a bank, or even an Internet service provider might all be targeted in some assaults. Behind these attacks, financial gain is one of the key motivations. Besides these targets, political administrations and governing authorities also attract the aggressor (Mahjabin et al., 2017).

5.1. Motivation for DDoS attack

DDoS assaults are carried out for a variety of reasons. The reasons for this are divided into five categories, which describe why an attacker attempts to get a server or network down (Devine, 2016; Nazario, 2008).

5.1.1. Intellectual challenge

Young enthusiasts who are looking to make a name are the main assaulters of this group. The would-be hackers with some technical acquaintances are motivated to persuade DDoS attacks in order to flaunt their knowledge and capabilities. Many botnet variants and utilitarian attacking tools are easily available in the market which incentivizes these attackers to experiment with DDoS. Their main targets are isolated devices and users (Ghali et al., 2020).

5.1.2. Monetary and economic gain

Attackers of this group attempt to gain some monetary or financial benefits, hence attacks of this category are considered the deadliest ones. The assaulters in this class are professionals and experts in their field. Thus, controlling these attacks is quite problematic (Mahjabin et al., 2017). When attackers target organizations, they may leave an extortion demand over them. At that

Table 2
Taxonomy of IoT Attacks, Security Challenges, and Requirements based on IoT Layered Architecture.

Layers	Attacks	Security Concerns	Requirements
Application Layer	• Phishing Attack (Akram et al., 2018) • Malicious Code Injection (Chen et al., 2018) • Information Leakage (Chen et al., 2018) • DoS/DDoS/WebDDoS Attack (Gupta et al., 2009) (Yu et al., 2021) • Intermediate Attack or Man in the Middle Attack (Hamza and Arshad)	• Data confidentiality • Integrity breach • Access Control • Authentication and Authorization	• Implementing various Authentication Algorithms • Key Arrangement • Privacy-Preserving Algorithms
Data Processing Layer / Middleware Layer	• Flooding Attack over the Cloud (Agrawal and Tapaswi, 2019) • Cloud malware Injection (Akram et al., 2018) • Signature Wrapping attack (Roohi et al., 2019)	• Processing of huge data • Filtration of the Legitimate Information	• Applying filters to detect the suspicious data • Protected Cooperative Communication • Secure Processing
Network Layer	• DoS/ DDoS Attack (Chen et al., 2018) (Hamza and Arshad) • Sybil Attack (Salim et al., 2020) • Sinkhole Attack (Hadhrami and Hussain, 2021; Akram et al., 2018) • Traffic Analysis (Mahmoud et al., 2015) • Replay Attack (Anand et al., 2020) • Sniffing Attack (Akram et al., 2018; Roohi et al., 2019; Hamza and Arshad)	• Network Congestion • unauthorised Access • Availability of Resources	• Secure Communication • Implementing Encryption Algorithms • Authentication Algorithm
Perception Layer	• Node Capture Attack (Mahmoud et al., 2015) • Malicious Node Injection Attack (Chen et al., 2018) • Eavesdropping (Pateriya and Sharma, 2011) • Sleep Deprivation Attack (Hadhrami and Hussain, 2021; Hamza and Arshad)	• Limited Resources Constraints • Vulnerable to Interference • Confidentiality, Integrity, and Availability of gathered data	• Light-Weight Cryptography algorithms • Devices' Identity Management

point, the assaulters force the victim organization to either pay the ransom or else expect a persistent threat from them in the future. As a result, paying the attackers will immediately help the organization. However, it also gives attackers the opportunity to strike again in the future (Zargar et al., 2013).

5.1.3. Revenge

Revenge is one more source of inspiration for DDoS outbreaks, in which some disgruntled individuals persuade the attacks in retaliation or to take revenge for alleged victimization. In this class, the attacker is perhaps technologically less proficient (Zargar et al., 2013). Corporations also launch DDoS attacks to disrupt their rivals and steal their customers. Attacking certain rivals would ensure the associations that the rival's clients would not be able to access their networks and resources and migrate to the assailant's services instead. When the victim refuses to provide services for an extended period, customers/clients lose faith in the organization's (victim's) ability to serve them. The best example of such practices is common among gambling websites (Nazario, 2008).

5.1.4. Ideological belief

A few assaulters are empowered to attempt the assault due to their philosophical conviction and they target the victim. DDoS assaults have become more prevalent as a result of this. Although they are not as common as other reasons, their effects and sizes are comparable to those found in recent years. A few of the widely publicized DDoS attacks over the last decade are the Estonia outbreak in 2007, 2008, and 2016 the China and CNN assaults, 2009 and 2017 the Iran DDoS attempt, and in the year 2010 and 2018 Wikileaks, many of which were motivated by philosophical or political convictions (Mahjabin et al., 2017).

5.1.5. Cyberwarfare

Cyberwarfare can be another prominent attack motive that poses a threat to its targets and has considerable economic consequences. An attack of this nature is usually carried out by a group of proficient members of a military or terror organization. The assailants, in this case, are from various countries and attack organizations from other nations. Govt-authorized DDoS attacks could be used to cripple all rival websites and networks of an enemy country. Armed groups or the forces of government occasionally emasculate their rivals, and attack, and deface the website of their representative or administration (Prasad et al., 2014). Such assaults require a substantial number of resources and time, and they have the potential to cripple a nation's cyber world and vital infrastructure by disrupting service. A lot of such attacks on countries like India, America, Thailand, South Korea, Japan, China, Russia, Pakistan, Brazil, and Georgia have also become Cyberwarfare casualties. In 2011, the Syrian Army emerged, supporting its president in attacking many Western media organizations and humanitarian organizations (Britannica, 2020).

5.2. Why attackers choose IoT devices (Salim et al., 2020)

DDoS attack techniques are becoming increasingly popular, with attackers preferring to persuade DDoS attacks through IoT devices. These devices lack critical safety procedures, which in turn make them easy to manipulate. The intruder may corrupt an IoT device

Table 3
Features of IoT Devices that Attract the Attacker.

Features Attracting the Attackers	Description
Globally Connected	As the term indicates, the Internet of Things refers to gadgets also named as the things that are always linked to the internet. It is a network of embedded distinct devices like telecommunication devices, household appliances, etc. These devices are accessible to all and are hardly ever turned off as it is an open network hence the intruder takes the advantage of that and infects them
Inadequate Security Measures	Many IoT devices do not have any security algorithms due to their size, storage capacity, and computational limitations. This creates security vulnerabilities and assailants use these to exploit the devices.
Unable to Change Authorization	Once the intruder gained control of a distorted IoT device, he/she is free to alter the device's security credentials and will utilize these corrupted devices to perpetrate as much damage as he can on the target. If the infected device is ever tracked during an attack, the owner or maker of the device will be unable to reclaim control from the attacker by resetting the security credentials.
Easy to Crack Passwords	Most of these gadgets have the default authentication credentials that the device manufacturer gave and the device user hardly changes the credentials. IoT devices frequently share the same user_id "root" and "password" as the factory-configured passcode. As a result of this attackers can quickly obtain access to such devices.
No Security Code Upgrades	The device manufacturer does not check the security credentials after the device is distributed to the market. Due to that, the software code of those devices may contain safety patches and loopholes. The attacker exploits these loopholes to persuade an attack. If any of these devices are damaged or faulty then the manufacturer does not provide any security upgrades to fix the flaws.
Cost-Effective	Besides being vulnerable to unauthorized access, IoT devices are inexpensive also. For a fraction of the cost of running a server, aggressors may manage faulty IoT devices instead of contributing and maintaining expensive servers.

and can propagate the malware to other devices as well, eventually forming a collection of infected devices and naming it a botnet (McDermott et al., 2018). Besides the common attack motivations discussed earlier, there are some other reasons for selecting IoT devices for attempting a DDoS attack are stated in Table 3:

In this section, we have discussed the reasons that inspire the assaulters to persuade an attack and why they target IoT devices to perform such attacks. The next section discusses how the attacker performs an attack over an IoT network after being motivated.

6. DDoS attack in IoT

IoT works on the principle of heterogeneity as it connects a billion users and devices to a distributed network which makes it more vulnerable to exploitation and security risks. There are numerous security threats to IoT out of which the most widely recognized are brute force assaults, botnet malware, and DDoS attacks (Anirudh et al., 2017). IoT trusts on network foundation for information transmission, and a DDoS attack can severely influence its competencies. DDoS makes the utilization of information inaccessible to clients. It additionally drove towards the compromise of power, bandwidth, transmission capacity, preparing, memory, authentication, and loss of information. The IoT devices are deficient in the assets which give privacy and authentication. The network infrastructure of IoT is comprised of wireless communication and wireless sensor technologies. It is the primary reason for the pervasiveness of DDoS assaults in IoT. IoT applications, for example, wireless body area networks, and numerous well-being applications are inclined to DDoS assaults because of the absence of capacity and restricted assets (Anand et al., 2020). The most significant loss that attackers provide through a denial-of-service attack is TCP SYN flooding (Gupta et al., 2009). The lack of security found in the perception layer starts the DDoS assaults. As the impact of a DDoS attack on IoT security is high, so many researchers are working on solutions. Some of the investigational studies are discussed in this paper. Fig. 4 shows a pictorial view of how a DDoS attack is performed:

6.1. DDoS attacks using IoT botnets

Attackers execute DDoS assaults against servers and networks using non-legacy IoT devices (Tushir et al., 2020). These gadgets have short battery life and less computational power which makes it easy for an adversary to invade such devices. For a DDoS attack to be effective, an aggressor must first create a botnet. Botnets are a group of non-legacy IoT devices that have been hacked and turned into malicious bots (Prasad et al., 2014). In addition to routers, Audio speakers with internet connectivity, Surveillance cameras, and webcams, non-legacy IoT devices include household appliances like web-enabled heaters, refrigerators, TVs, and home security schemes. Botnet outbreaks against non-legacy IoT gadgets are possible due to their faults and inefficient built-in security. An attacker utilizes a brute-force approach to break the cryptographic authentication algorithms and obtain access, which undermined the devices' security. Frequently, IoT device makers design products using the same passcode for most of them. An attacker who knows the authentication credentials of a single node then he/she can get access to a large number of unprotected devices (Salim et al., 2020). The IoT device owners are not aware of the fact that their device is already hacked. On the other hand, the attacker has access to the systems, and then he executes a DDoS assault by sending packets from a large number of disrupted devices against the target. Because the source of the broadcast comes from unsuspecting and authenticated users, hence the attacker does not need to fake the address of the packets delivered (Aamir and Zaidi, 2013).

6.1.1. How attackers create a botnet

IoT bots are an accumulation of smart Internet of Things devices that cyber-criminals have taken over to attempt a DDoS assault. Botnets are often built according to a pre-determined strategy. It is a campaigner, a solitary individual, or a group of programmers cooperating with a criminal organization, that programs the code to contaminate the devices. This malware can sit on a gadget that can execute code; however, programmers can likewise make it explicitly target IoT devices. After developing the malicious program, the assailant utilizes it to corrupt as many devices as he can to form a botnet with these hacked devices (Pratt, 2020) (Kashyap and Jain, 2021).

The process of using an IoT device as a botnet and then performing the attack involves the following four steps:

(1) Capture: Recognize and gain access to IoT devices.
(2) Subvert: Modify the device's code to perform malicious activities.
(3) Activate: Direct the distorted device to persuade the attack.
(4) Attack: Execute the DDoS assault.

In terms of composition, IoT botnets are quite similar to traditional botnets. IoT botnets are made up of two main components.

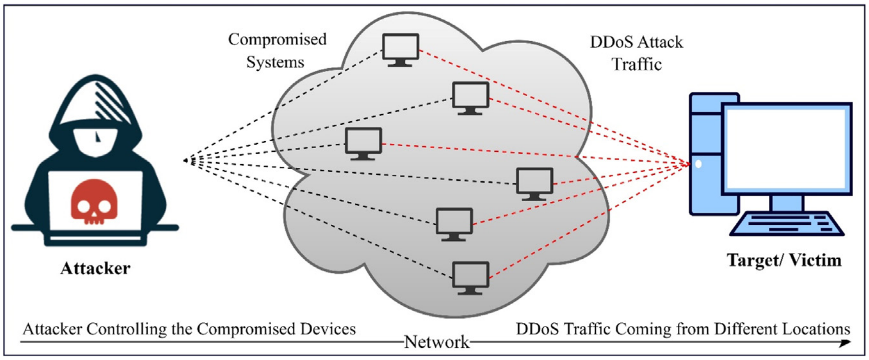
Compromised Systems
DDoS Attack Traffic
Attacker
Target/ Victim
Attacker Controlling the Compromised Devices
Network
DDoS Traffic Coming from Different Locations

Fig. 4. How DDoS Attack is Performed.

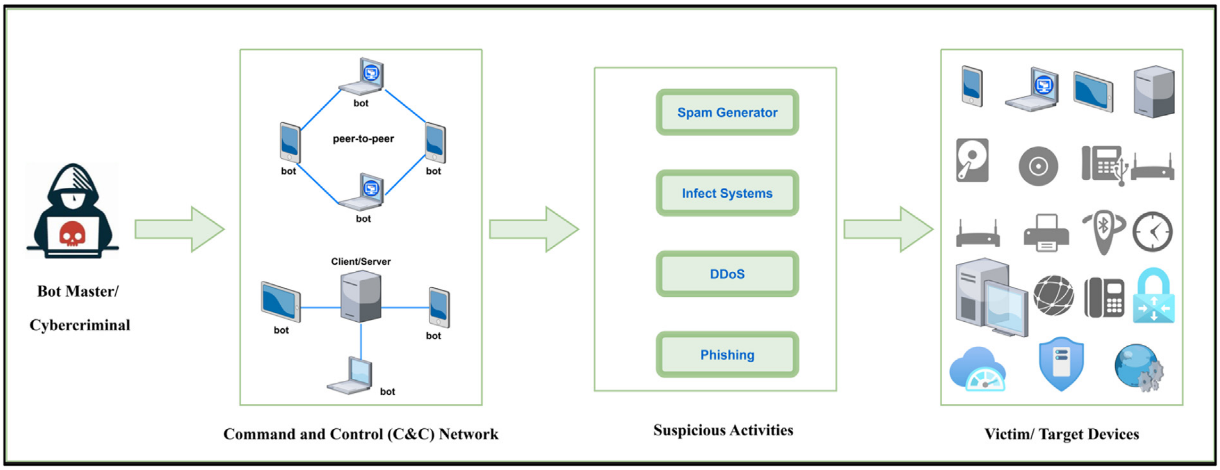

Fig. 5. Botnet Command and Control Architecture (Pratt, 2020).

The first component is the C&C server or controller or handler (McDermott et al., 2018), from where the cybercriminals manage the botnet while the second involves those systems that have been hacked or infected independently as shown in Fig. 5.

Cybercriminals exploit the strength of compromised systems in a botnet to perform malicious activities like Distributed Denial of Service (DDoS) assault. Nowadays, DDoS attacks have grown stronger as cybercriminals use giant botnets made up of weak IoT computers. Specialists have cautioned for years about the vulnerabilities of connected devices. Malware-threatening IoT botnets have become much more complex, and now involve exploits for identified vulnerabilities and safety bugs in zero-day. Some services provide botnets for rent also. The provider rents its resources to anyone who wants to break an online platform or disable it, charging for the time and power of that attack. Quite a lot of botnet assaults have occurred in recent years, some of the popular botnets are:

(a) **Linux.Hydra:** Linux.Hydra has first arisen in 2008 as open-source and easily accessible software and was particularly intended for routing devices with MIPS (Microprocessor without Interlocked Pipelined Stages) architecture. Most IoT malwares have their origin in Linux.Hydra. When the target device is a D-Link switch, the exploitation step is based on a dictionary attack or a specific and well-known authentication weakness. When the assailant distorts a device, the IRC-based network executes the fundamental SYN flood attack. According to the malware literature, this also permits the attacker to attempt a UDP Flood attack, although sources on the internet do not demonstrate this. No matter how simple it may seem but this malware put down the foundation for future MIPS-pointing malware (Donno et al., 2017).

(b) **Psyb0t:** Linux.Hydra and Psyb0t are quite similar. The Psyb0t malicious program has come into consideration since the beginning of the year 2009. Psyb0t can also execute UDP flood attacks as well as ICMP Flood attacks, unlike its predecessor. Although one cannot compare the two malwares directly because the origin of both has not yet been revealed. But they have so many similarities that it is fair to conclude that Linux.Hydra is an antecedent of Psybot malware (Durfina et al., 2013).

(c) **Chuck Norris:** Chuck Norris came into sight in 2010 after the developer of Psyb0t botnet brought it down. There are quite a lot of similarities between Chuck Norris and Psyb0t, and at that time, this was most possibly the Psyb0t's immediate progression. Apart from the lack of an ICMP Flood attack, which is replaced with the ability to carry out an ACK Flood, the remaining available attacks are the same (Celeda et al., 2010).

(d) **Tsunami/Kaiten:** It is a combination of both the Kaiten-Tsunami DDoS tool and Chuck Norris, the last and most grounded descendant of Hydra. Specifically, this malicious software has several characteristics similar to the previous malware, such as a similar encryption key and certain CNC IP addresses, among others. With the help of Tsunami, botnet zombies are able to deliver not only traditional SYN flood attacks but also more complex ones like HTTP Layer 7 Flood and TCP XMAS attacks. Strangely, in 2016, this malware was purposefully snuck into the Linux Mint Official ISO, putting a large number of freshly released OSes in danger (Donno et al., 2017).

(e) **BashLite:** IoT devices such as cameras and DVRs (Digital Video Recorders) that run Linux are particularly susceptible to this type of malware. With this botnet, DDoS assaults such as UDP and TCP flooding attacks, as well as an HTTP attack with a bandwidth of 400 Gbps, may be launched. Some other names of this malware are Lizkebab, Torlus, and gafgyt. The strategy of the arrival of this botnet is unique because it does not rely on potential vulnerabilities (Micro, 2019). Instead, it exploits a Metasploit module, which is freely available for remote code execution (RCE). In 2015, developers had access to the source code which allowed them to enhance the software.

(f) **Mirai:** Mirai has been the most common IoT malware since its inception in 2016 and continues to grow. Security cameras, Home routers, Baby monitors, and other such household IoT gadgets were the most probable victims of this malware among other devices. Mirai hacked these devices using the first list of 64 frequent usernames and passcodes because of the minimal or weak security on these devices (Jerkins, 2017). The analysis done by Imperva Incapsula shows Mirai is able to create an HTTP flood attack and several network-level attacks. Mirai is hard-wired to exclude IP address sets, such as those owned by General Electric, Hewlett-Packard, and the United States Defense Department (Kolias et al., 2017). Upon contaminating a computer, Mirai searches for and wipes out other malware on that system to claim the device as its own. As the source code of the Mirai botnet was public and accessible to everyone, attackers created new malware variants continuously by changing a lit bit of Mirai's code (Micro, 2019).

(g) **Remaiten:** Raemaiten was first seen in 2016. Tsunami's DDoS characteristics were added, while BASHLITE's scanning capabilities were updated and enhanced. Remaiten enhances its spreading process with the help of downloader executable code that is widely used in Linux-based devices for CPU architectures i.e., Remaiten can download an executable file and can get access to the IoT devices. After gaining access to IoT devices, it is possible to execute architectural-style assaults. Then these binaries are executed on the new victim device, producing another bot to be added to the botnet by malicious operatives (Micro, 2019). In the complex IoT system architecture, Remaiten is acclaimed for its complexity and adaptability.

(h) **3ve:** It was a composite of three distinct but connected sub-operations, each of which committed ad fraud and was skilled at evading discovery. 3ve created billions of fraudulent ad bid requests using its diversified and complicated system (i.e., ad spaces on websites that promoters may automatically bid for purchasing). It also produced millions of fake, fraudulent domains. In 2018, White Ops, Google, and Law enforcement agencies conducted an investigation that resulted in an unprecedented takedown of the botnet. The network of this botnet started small but developed into a large botnet that dominated a vast number of IP addresses in residential and corporate domains over a period of two years. 3ve was distinct from previous botnets because it could self-create a botnet by making fake copies, masquerading IP addresses with proxies, and hijacking the IP address of the Border Gateway Protocol (BGP) in terms of selling fraudulent ad inventory to advertisers to raise profit (Vishwakarma and Jain, 2020).

(i) **Wirex:** The WireX botnet was discovered in August 2017, after firms in a variety of sectors, most particularly hospitals, gambling sectors, and even some domain registrars showed signs of major distributed denial of service attacks. In the command-and-control (C&C) protocol, it is called on one of the delimiter strings. It also included thousands of Android devices which had apps that appeared genuine but were malware in actuality. Most of those applications concerned were multimedia players, memory managers, or widgets. After they had compromised a computer, they called out for attack instructions to a command-and-control domain. Even if they were running in the background on an Android device, the applications used device resources and were able to initiate attacks (Bhuyan et al., 2015).

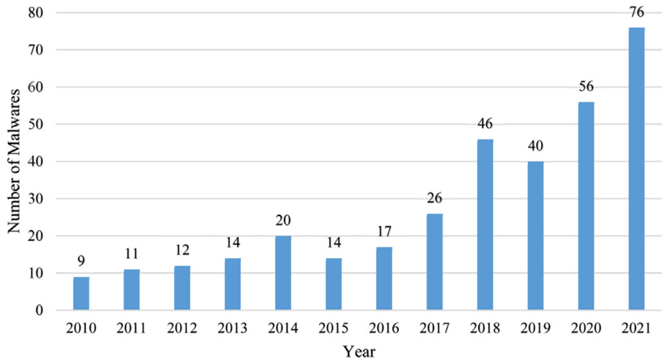

Fig. 6. Increment in the Number of Linux-Based Malwares from 2010 to 2021 (Intezer, 2021; Toulas, 2022).

To fight this botnet some big companies came forward, companies such as Akamai Technologies, Flashpoint, Google, Oracle Corporation, and Cloudflare. Google took extra prevention and withdrew thousands of malware applications from the Play Store.

(j) **Reaper:** While Mirai caused massive disruptions, it simply exploited poor or default passwords to affect IP cameras and network routers. The new botnet hazard is alternatively known as the IoT Troop or Reaper. Reaper has developed the tactic by utilizing the actual application hacking methodologies to get control over the computers. The Reaper malware has compiled several IoT hacking strategies, including nine attacks against D-Link, Netgear, and Linksys routers, as well as digital surveillance systems offered by firms including Vacron, GoAhead, and AVTech (Greenberg, 2017). This IoT botnet is an improvement of some of Mirai's code sections. Instead of simply interpreting the login details of the systems it penetrates and exploits known potential vulnerabilities in the scripts of infected devices. Using several intrusion methodologies to get access it subsequently grows and creates a larger botnet.

(k) **Torii:** Dr. Bontchev has discovered Torii on his honeypot through 'Tor' exit nodes and hence this is named 'Torii'. This malware had the option to victimize the majority of those current systems, cell phones, and tablets that have x86(64-bit), x86, ARM, MIPS, and so on architectural models. It looks for a Telnet port to bypass the weak authentication of the device as the Mirai does. But it is more sophisticated than most other IoT malwares because of its ability to move the appropriate payload to contaminate others with similar models (Vishwakarma and Jain, 2020).

(l) **Meris Botnet:** Meris is a new DDoS botnet variant that is comprised of nearly 30 thousand disrupted systems/devices. Meris has another term in Latvian as "Plague". This botnet is created from an advanced device that is needed to function with an ethernet connection. Some key features of Meris while persuading an attack include the use of HTTP Pipelining, an open port 5678, and a proxy. The botnet crashes the servers in order to carry out a massive DDoS Attack (Raza, 2021; Shapelez, 2021).

Most of the attacks are carried out by using Linux-based malwares and botnets. These malwares are increasing tremendously by each year. Fig. 6 shows this increment of Linux-based malware from the year 2010 to 2021.

6.1.2. Botnet distribution geography in Q4 2021

The US has always been the traditional leader in terms of C&C server facilitating (46.49%), and the final quarter of 2021 was no exception. Germany (7.02%) and the Netherlands (10.17%) won silver and bronze in the fourth quarter of 2020 and they hold their

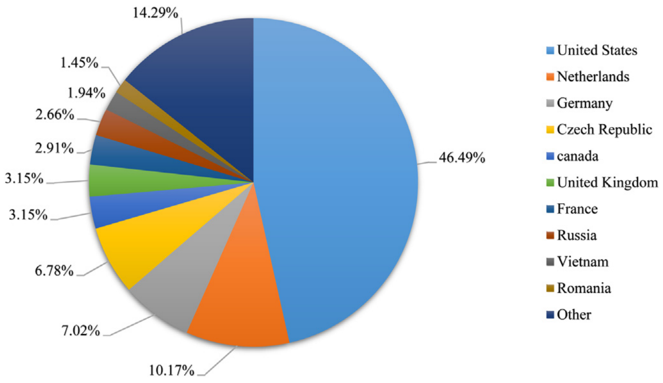

Fig. 7. Botnet C&C Servers Distribution by country in the Final Quarter of 2021.

places in the final quarter of 2021. The Czech Republic grew its shares by 3p.p. having 6.78% CC servers. Canada and the United Kingdom reserved fifth place with 3.15% of CC server distribution. France (2.91%) fell for the sixth position trailing Russia (2.66%), Vietnam (1.94%), and Romania with 1.45% (Gutnikov et al., 2021). The geographical distribution of Botnets is depicted in Fig. 7.

6.2. The architecture of DDoS attacks

The general architecture of a DDoS attack consists of an attacker/ a group of attackers, controllers/botnets, and a target/ victim. The Botnets that are geographically distributed make this attack a distributed DoS attack. The aim of the attackers is to disrupt the service of the target server. The attackers give commands to controllers (Handlers) who control the Botnets (Aamir and Zaidi, 2013). The commands include the type of attack, time of the attack, duration of the attack, etc. Most of the time, the botnets are used by the botnet providers. The infected IoT devices then send spurious requests to the server (victim). Sometimes, an infected bot is also used to further spread the malware to its network, to make more infected bots for the attack. This increases the strength of the botnet exponentially and the capability of the botnet increases multifold. In Section 6, we have discussed how a botnet is created and how the attack is persuaded. When designing a DDoS attack, it is really important to consider how the various actors interact. A DDoS attack can be carried out using one of four types of network architectures namely: Agent-Handler model, Reflector model, IRC-based, and Web-based models (Donno et al., 2017).

6.2.1. Agent-Handler model

The Agent Handler model consists of clients, handlers, and agents as depicted in Fig. 8. Attackers use the clients or customers to communicate with the handlers or masters. These handlers are programmed software bundles that are situated somewhere over the internet. These packages contaminate the network assets and transmit data from the customers to the specialists or handlers (Sonar and Upadhyay, 2014). On compromised systems, the agent (which is a program block') executes itself and launches the attack against the ultimate target. Similar to the contaminated machine, the phrase "agent" refers to the code that is running on the computer system. Depending on how the network architecture is set up, a botnet (a group of agents) can work with a single handler or multiple handlers (Prasad et al., 2014).

6.2.2. Reflector model

The Reflector model is pretty much identical to the Agent-Handler model, the Fig. 9 shows an additional set of noncontaminated systems called reflectors. By using handlers, the reflectors are made to send a stream of packets to the victim. They often use a fake IP address to request that the reflectors send replies to their victims. Consequently, the target host receives a large amount of network traffic as a result of this. As an amplifier, the reflectors are often used to send packets to the broadcast addresses of the reflector network and then trigger reply packets out of each node inside the LAN (Donno et al., 2017). The attacker does not need to infect a reflector, which can be any host on the Internet that can respond to IP requests, for example, a web server that communicates to TCP SYN requests. Distributed Reflection Denial of Service (DRDoS) (Tao and Yu, 2013) attacks use this model and are more difficult to detect back than any of those relying on the Agent-Handler Model of DDoS attacks.

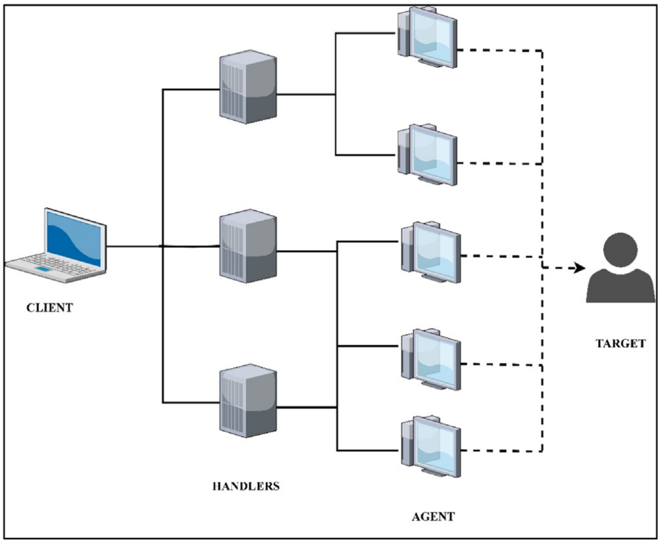

Fig. 8. Agent-Handler Model.

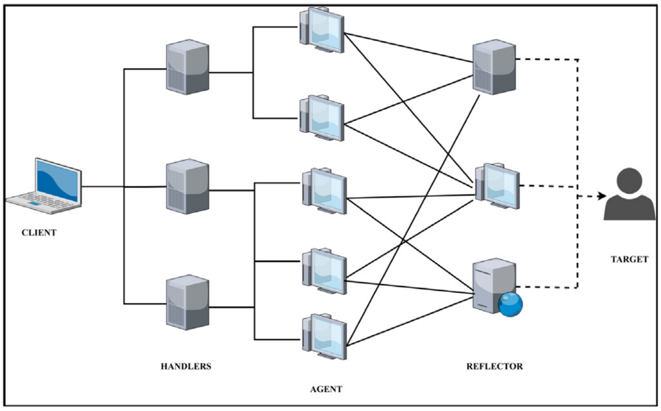

Fig. 9. Reflector Model.

6.2.3. Internet Relay Chat-based (IRC) model

The IRC model is much similar to the Agent-Handler model, but the client communicates to agents via an IRC-based transmission medium rather than handlers, as depicted in Fig. 10. As a client/server textual protocol, Internet Relay Chat (IRC) can be utilized to implement a multi-user and multiple-channel chat system (Jerkins, 2017).

6.2.4. Web-based model

This model is closely related to the IRC-based model, but the exchange of information is HTTP/HTTPS-based. Furthermore, the majority of the agents are completely configured and constrained

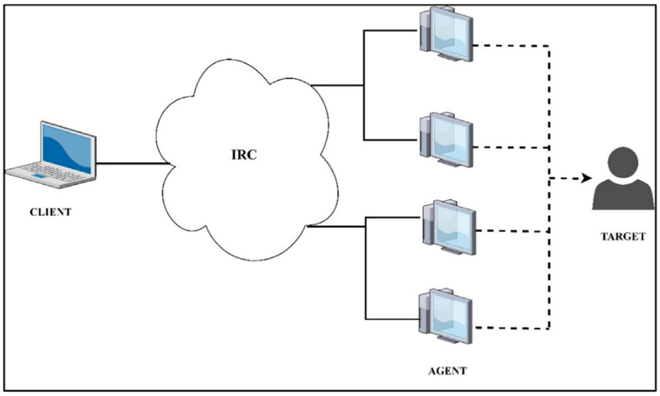

Fig. 10. IRC-Based Model.

via complex PHP scripts and encoded communication, whereas other agents are mostly used to update the statistical data to a monitoring website (Zargar et al., 2013).

6.3. Taxonomy of DDoS attacks

There are numerous sorts of DDoS assaults that can be implemented presently, and a variety of classification systems have been suggested. During the past few years, DDoS attacks have evolved in terms of their attack methods, and there are still many possibilities to be explored (Zargar et al., 2013). IoT explicit DDoS attacks and conventional DDoS attacking strategies are not much different from each other. In order to exploit the vulnerabilities in conventional systems or IoT devices, they use similar techniques (Shah and Venkatesan, 2019). Distributed Denial of Service attacks are generally classified into three categories as shown in Fig. 11. The following-mentioned attacks are distributed in the application, network, and transport layers (Hamza and Arshad).

Along with the mentioned variants of DDoS attacks an application layer (L7) DDoS attack is evolving. Attackers attempt these attacks by using multiple emulation dictionaries. In this attack, the intruder emulates a legitimate user's request patterns by flooding the victim's site with a large number of requests. The attacker creates some lists with request patterns imitating the legitimate user's requests and then commands the bots to use these look-a-like patterns. This process may be attempted using two scenarios where either the bots will use the same emulation dictionary or different dictionaries distributed over different locations (Cirillo et al., 2021).

There are several types of attacks imaginable with the help of IoT devices in IoT-oriented environments, such as the cloud which is central to the provision of relevant user services (Sharafaldin et al., 2019). The attacks that can happen on the cloud are classified into two categories Bandwidth depletion attacks and Resource depletion attacks or Reflection based and Exploitation based attacks (Jia et al., 2020) which are shown in Fig. 12. The purpose of the bandwidth depletion attack is to use an attacking army i.e., botnets absorb the complete network bandwidth. The attempt takes place by amplifying or transmitting a large numeral of spoofed packets to maximize the outbreak. Further, we can classify the Bandwidth depletion attack into two categories, Protocol Exploit attacks and Amplification attacks (Mahjabin et al., 2017).

In a resource depletion attack, users are not able to use their CPU, socket, and memory. The resource depletion attack takes place by transmitting malicious packets to the target (Mahjabin et al., 2017). The Ping of Death attack or exploiting vulnerabilities in the victim's device, network, application, or transport layer protocols are examples of resource depletion attacks (Sonar and Upadhyay, 2014). Attackers exploit the weakness of different protocols of IoT layers to launch the DDoS attack. For example, in the UDP flood attack, the attacker overwhelms/floods the host (victim) random port with User Datagram Protocol packets. The host (victim) continuously checks for the application listening to that port that no application belongs to that port in actuality. In response, the host sends an ICMP Destination Unreachable error message. This process consumes host resources that will lead to the unavailability of the host to its legitimate users. Protocol Attacks (which take place by hampering the protocols) such as Ping of Death (PoD) and Smurf manipulate Internet Protocol to send malicious pings to a system. The most dangerous of these is a DDoS attack (Zhang and Green, 2015).

Attackers use the Ping Scan technique to discover possible victims, and the most known Ping Scans are the UPD, TCP SYN or ACK, and ICMP. ICMP scan is effective when Firewall and ACL rules are less restrictive against LANs or a range of Internal IP addresses. However, UDP Scan is useful when unsolicited UDP traffic and egress ICMP traffics are not blocked in the Firewall. In the case of TCP, scan effectively against a stateless firewall that doesn't reject unsolicited ACK packets (Mahjabin et al., 2017).

DDoS outbreaks can also be categorized based on the protocol used for performing the attacks. Broadly these are classified into three classes that are TCP-based, UDP-based, and ICMP-based attacks (RioRey, 2015).

All the specific attacks are discussed in the following subsections with a brief description:

a **SYN Flood Attack:** TCP protocol uses a three-way handshake method for establishing a connection between two devices. The mechanism uses three types of packets that are SYN, SYN-ACK, and ACK. In an SYN flood attack, the attacker initiates multiple connections by continuously sending the spoofed synchronization frame but does not finalize them. As a result, the server leaves the ports open for the acknowledgment frame (Ubale and Jain, 2018). Thus, the connection is termed half open and the attack is termed a "Half Open attack". Consequently, the SYN flood overwhelms the victim server by depleting its framework resources which is the connection table memory that is generally utilized for storing and processing these incoming packets (Ghali et al., 2020). As a consequence, this degrades the performance of the network or completely crashes the server. In order to protect against large-scale SYN floods, one can use the SYN–Cookie defense methodology. However, the approach requires all servers to support this capability (Gupta et al., 2009).

b **SYN-ACK Flood Attack:** During the TCP handshake, when the host receives a SYN request packet it will revert with a SYN+ACK packet as a server response. To execute this sort of assault the assaulter overloads the target machine with SYN +ACK response packets.

It is possible that this attack will cause a high rate of spoofed SYN+ACK packets on the server. The server uses its resources like memory, CPU, and many others to mitigate this unusual behavior but cannot handle the network congestion created by response packets (Prasad et al., 2019). As a result, the server faces denial of service or a complete server shutdown (Zargar et al., 2013).

a **ACK & PUSH ACK Flood Attack:** In this attack, after the establishment of a TCP-SYN session between the host and the user, they communicate through ACK and PUSH-ACK frames until the session continues. During the ACK flood attempt, the target receives a high packet rate of spoofed ACK frames that do not refer to any connection list of the server. In order to match these frames, the resources of the target's server are depleted by the

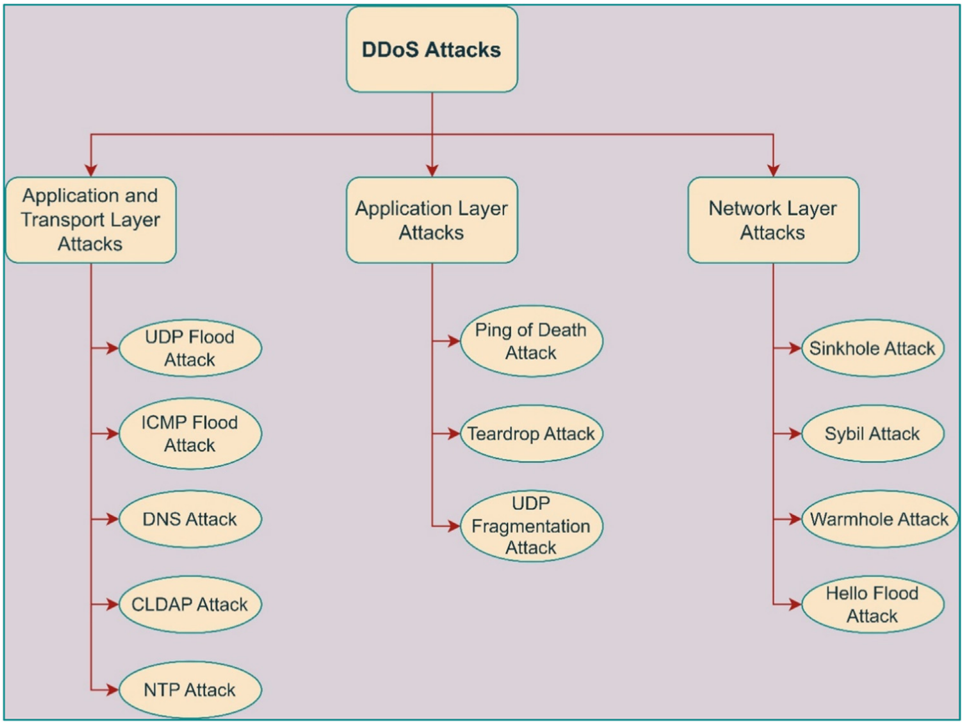

Fig. 11. Classification of DDoS attacks based on the different IoT layers.

ACK flood attack which causes degraded performance and/or closes the server completely (RioRey, 2015).

b **Fragmented ACK Attack:** The fragmented attack is a version of the ACK and PUSH-ACK Flood assault. For producing a normal or moderate packet rate the attempt utilizes a 1500B size frame that consumes a lot of the network bandwidth (Javapipe, 2016). The frames or packets normally pass through the ACLs, Switches, Firewalls, IDS, and IPS because the router does not reassemble the fragmented frames. The packet contains a lot of randomized and irrelevant information. The assailant's primary goal is to consume the victim's whole bandwidth. All servers in the victim's network will get affected by a fragmented ACK attack (RioRey, 2015).

c **RST or FIN Flood Attack:** The client and host servers exchange RST or FIN packets for terminating the TCP-SYN session. This process uses a Three-way or Four-way TCP handshake. RST or FIN floods cause victim servers to receive large numbers of spoof RST or FIN packets that do not belong to any particular session in the server's database, causing them to crash. When the victim's server is hit by an RST or FIN flood, its system resources get destroyed while trying to match these incoming packets. Which results in a complete server shutdown or system performance degradation (RioRey, 2015).

d **HTTP Fragmentation Attack:** Here, a non-spoofing BOT creates a legitimate HTTP connection with a remote server. According to the researchers, while fragmenting genuine HTTP packets, the bot sends each fragment as slowly as the server timeout permits, causing the HTTP connection to hold for a lengthy period without raising any warnings. HTTP session time can be prolonged for Apache and other web servers with inefficient time-out methods, resulting in an extremely lengthy HTTP session time. It is possible for an attacker to halt a web service using just BOTs by initiating numerous extended sessions per BOT (Kotey et al., 2019; Ghali et al., 2020).

e **UDP Flood Attack:** In a UDP flood attack, unknown or spoofed UDP packets are sent to a target server at an extremely high rate with a wide variety of source IP addresses. Incoming UDP packets overwhelm the target server. The assault exhausts the network's resources and bandwidth, causing it to shut down. Due to the lack of a full communication handshake in UDP while data transfer, UDP assaults are hard to trace and thus very good at flooding the network. Using the victim's information as the Destination port and IP address, UDP floods can overrun a network with packets that include randomized or consistent Source IP addresses (Vishwakarma and Jain, 2020; Chickowski, 2020).

f **UDP Fragmentation Attack:** This assault is an adaptation of the UDP flood. Using big packets (1500 bytes), the attacker is able to use more bandwidth while sending fewer messages. Because these frames are faked and have no genuine relationship between them, the target server will waste CPU resources while trying to "reassemble" the worthless packets. This can cause the CPUs to overheat which in turn results in a system reboot. Due to the fact that it looks like normal traffic, this assault is difficult to detect (RioRey, 2015).

g **DNS Amplification Attack:** DNS amplification attack comes under the reflection-based DDoS assault categories. The attack is easy to persuade because it uses UDP packets and unlike TCP it does not rely on a handshake. Because of this, the source IP validation can be avoided. Attackers use the open DNS resolvers to overload the target's machine with DNS responses (Molvizadah, 2016). The assaulter sends spoofed DNS requests that seem to be legitimate to a DNS server and when the resolver responds to them the response frame is sent to the victims' system. The assault is called an amplification attack because the DNS server is bombarded with a number of 'DNS ANY' request queries and the response to this query increases the payload size of the response packet which in turn congests the victim's bandwidth. When the server is flooded with request packets it is unable to tell which packet is coming from a genuine system, therefore it responds to all requests regardless of the source. As a result, it depletes the network's resources

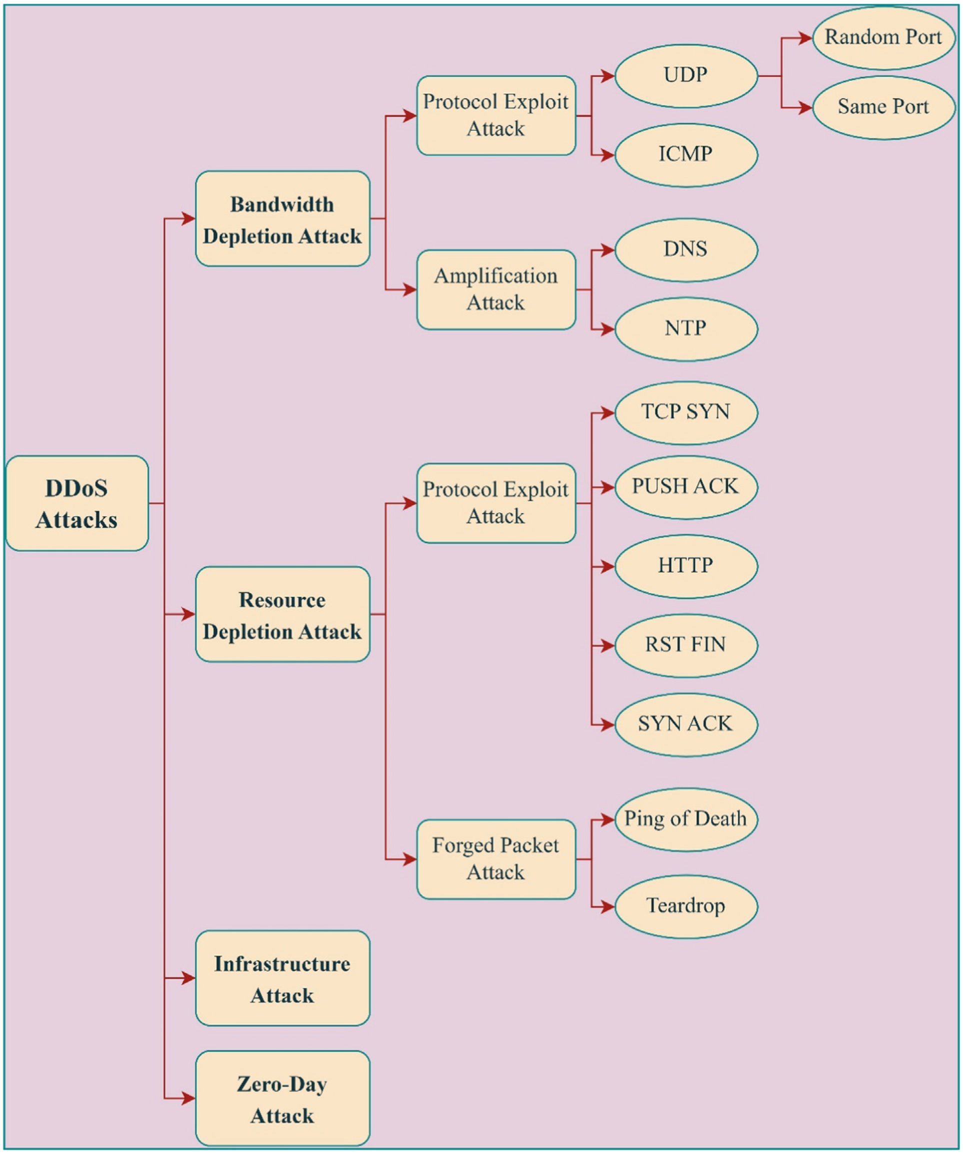

Fig. 12. Taxonomy of DDoS attacks on IoT Cloud.

and bandwidth, causing it to shut down (Srinivasan et al., 2019). This attack is undetectable by deep packet inspection since the packets are completely normal in appearance. Using a variety of IP addresses, the attacker may easily avoid detection by most traffic anomaly detection technologies (Afek, 2016).

h **Non-Spoofed UDP Flood Attack:** In this exploit, a target server gets non-spoofed UDP packets at a quite higher transmission rate and becomes overloaded by a huge number of UDP packets. The assault depletes system services and transmission power, eventually causing the network to stop working. The source IP address of Non-Spoofed UDP Flood packets is the real public IP address of the aggressor BOT, and the source IP address range corresponds to the number of BOTs deployed in the attempt. Because it mimics legitimate communications, this sort of attack is more difficult to detect (RioRey, 2015).

i **NTP Amplification Attack:** NTP amplification attack also falls under the reflection-based DDoS assault categories. In the NTP Amplification attack, the attacker uses User Datagram Protocol (UDP) packets to target the publicly available Network Time Protocol server. The Network Time Protocol is mostly used to sync the internal clocks of internet-connected devices (Rudman and Irwin, 2015). The command that can be used to start an attack on the server is the “MONLIST” command (Elleithy et al., 2005). The request packet for the MONLIST command is much smaller in size which is 64 bytes. While the reply of MON_GETLIST or MONLIST command is much higher when compared to its request packet size. Similar to DNS amplification, NTP amplification also uses UDP packets which are easy to spoof and hence make it a suitable asset for performing the DDoS attack (Czyz et al., 2014).

j **ICMP Flood Attack:** In this attack**, s**poofed ICMP packets arrive at a very high packet rate and from a very wide variety of source IP addresses on a victim’s server. The target server is flooded with inbound ICMP packets in enormous numbers. Network resources and bandwidth are depleted by the assault, as a result of which the network gets close (Srinivasan et al., 2019). The ICMP software stack does not perform a full communication handshake while exchanging the information making the ICMP-based assaults harder to detect. Overloading a network with random or fixed Source IP addresses is one of the dangers that an ICMP flooding attack generates. For example, the destination port and IP information of the victim might be used to send ICMP floods to a certain server (Aamir and Zaidi, 2013; Vishwakarma and Jain, 2020).

k **ICMP Fragmentation Attack:** On the other hand, the target server is bombarded with huge, fragmented, ICMP packets (1500 bytes) that cannot be reassembled while executing this assault. An ICMP attack's bandwidth is increased by the large payload size. In addition, it wastes CPU resources by attempting to reassemble worthless frames, which leads the target CPU to lose its resources. This type of attack might destroy and reset the victim's server (RioRey, 2015).

l **Ping Flood Attack:** This is an application-specific ICMP flood attack variation. While under attack, the target server is flooded with very high packet delivery rates and IP ranges from which fraudulent Ping (IMCP echo requests) are being sent. Incoming Ping packets will overload the target server as a result the network resources and transmission power will be depleted by the assault. If an attacker wants to fake a victim's IP address, he/she can use a random source IP. It is difficult to identify a "PING flood" using deep packet inspection or malicious behavior detection systems since the PING requests are generally well-formed and come from a large number of source IP addresses (Prasad et al., 2019; Javapipe, 2016).

m **Zero-day Attack**: A zero-day assault occurs on the first day or the 0th day of the program code after completion, utilizing undiscovered security flaws. As a result, the vulnerabilities of the system are known on day one following an attack on day zero. This is why it is termed zero-day. To encourage people to disclose zero-day vulnerabilities, several security groups and private software companies provide incentives and prizes. Before the assault is conducted, neither the impact nor the signature of this sort of attack can be known for certain (Mahjabin et al., 2017). Hackers prefer to use unexposed servers to create botnets for launching an effective DDoS attack and Zero-day vulnerabilities are a great choice for server attacks. Therefore, intruders employ this approach to get access to the server having these weaknesses, and thus they can get rid of the need for more bots. Once a server starts working as a bot, it may be used to carry out DDoS and other similar attacks as well (Oyekunle, 2021).

n **Infrastructure Attacks:** When it comes to DDoS attempts infrastructure assault is the most devastating form of it. In this attack, the goal is to cause major harm to the Internet. Hence, it targets both the network bandwidth and the resources (memory and CPU) of the victim's machine. Examples of infrastructure attacks include DNS, particularly root-DNSs, which are the top hierarchical service ports that offer services to all Internet users across the world. Because the DNS has a hierarchical structure, an assault of this sort that targets only the root name servers would not have a significant impact on the Internet service for the entire world. Attackers commonly employ DNS flooding tactics to initiate the assault, but other methods have been used. According to the attacker, this software is meant to infect IoT devices and execute DDoS assaults depending on their instructions (Mahjabin et al., 2017).

Although every type of DDoS variant damages the network and its resources. However, to be specific the amplification attacks and fragmentation attacks are hard to detect because in amplification attacks the request packets look like legitimate ones, and the response packet size is larger enough to destroy the victims' machine. Similarly, in fragmentation attacks, the fragmented packets can easily bypass the security mechanisms implemented over the routing devices and thus create trouble in the detecting process. The flooding attacks are somehow manageable by tracking the traffic continuously but that does not make them less dangerous. Moving forward the Zero-Day attack can be considered the most harmful one because it works on the new vulnerabilities of the software that are unidentified.

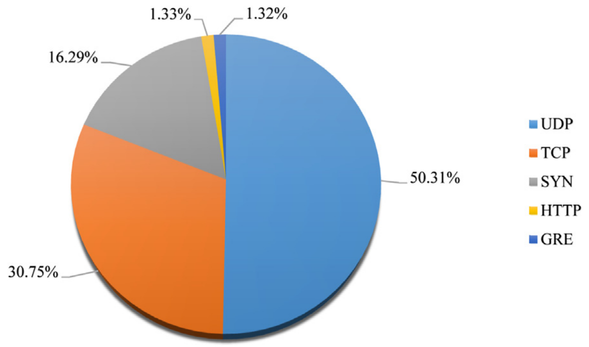

Fig. 13. DDoS Attacks Distribution by their type in 2021 Quarter 4.

6.4. Analysis of different DDoS attacks

Table 4 provides a comparative analysis of different types of DDoS assaults based on the protocol used by the attacker to perform the assault, the nature of the IP address which tells us if the packet is forged or not, packet size, transmission rate to get an idea about the pace the attack can be performed, and some recent tools (Ferrisbuller, 2022) which are easily available to anyone. The attackers use these to launch the attack effectively and intensely.

Table 4 compares the distinct variants of the DDoS attack performed using a few parameters. We may also use some other parameters like the amplification factor which is used to enlarge a packet to increase the attacking power or intensity of an attack. The amplification factor used in the DDoS amplification attempts like DNS amplification, UDP amplification, NTP amplification, etc (Vasques and Gondim, 2019). Another parameter that can be used is packet entropy, which is used to calculate the randomness of attributes such as source IP address and TTL value in a packet header. This packet entropy is calculated by using a series of continuous packets to find out the randomness in their source IP addresses. This calculation observes a significant change when the network faces an attack (Li et al., 2007).

6.5. Current statistics of various DDoS attacks

According to the trend illustrated in Fig. 13, the distribution of assaults by type continues to shift in 2021. When it came to the final quarter of 2021, the victorious leader, SYN floods (16.29%), lost its hold. UDP (50.31%) and TCP floods (30.75%) have been increasingly popular among attackers recently. As a result, GRE (1.32%) and HTTP flooding (1.33%), which made a place, also saw small increases. However, compared to Q3 2020, in 2021 there were more assaults based on UDP protocol than SYN flood (Gutnikov et al., 2021).

7. Defense mechanisms for DDoS attacks in IoT

With these advanced DDoS attacks, we need to come up with the same level or even higher level of defense mechanisms. While detection of an attack is not enough for stopping the attack, it is the first step toward defense. Other than the detection of DDoS attacks, there are two other steps required for the complete defense of the IoT network (Cvitic´et al., 2021; Srinivasan et al., 2019). Prevention of attack is the very first step of defense against DDoS attacks. Because of the FBI's decision in December 2018 to shut down 15 of the major DDoS sites, DDoS assaults, both in magnitude and quantity, have been on a decreasing trend (Crane, 2019). Prevention makes sure that the DDoS attack does not harm the system,

Table 4
Comparative Analysis of Various DDoS Attacks (RioRey, 2015).

Attack Type	Protocol Used	IP Address Nature	Range of Source IP	Transmission Rate	Size of a Packet	Tools used by the Attackers
SYN Flood Attack	TCP	Spoofed	Large	High	Small	DDoSIM, LOIC, HOIC, XOIC, Hping3
SYN+ACK Flood Attack	TCP	Spoofed	Large	High	Small	DDoSIM, LOIC, HOIC, XOIC, Hping3
ACK and PUSH+ACK Flood Attack	TCP	Spoofed	Large	High	Small	DDoSIM, LOIC, HOIC, XOIC, Hping3
Fragmented ACK Attack	TCP	Spoofed	Large	Moderate	Large	DDoSIM, LOIC, HOIC, XOIC, Hping3
RST and FIN Flood Attack	TCP	Spoofed	Large	High	Small	DDoSIM, LOIC, HOIC, XOIC, Hping3
HTTP Fragmentation Attack	HTTP	Non-Spoofed	Small	Very low	Small	PyLoris, HULK, RUDY, XOIC, GoldenEye
UDP Flood Attack	UDP	Spoofed	Very Large	Very High	Small	PyLoris, LOIC, HOIC, XOIC
UDP Fragmentation Attack	UDP	Spoofed	Moderate	Very High	Large	PyLoris, LOIC, HOIC, XOIC
Non-Spoofed UDP Flood Attack	UDP	Non-Spoofed	Small	Very High	Small	PyLoris, LOIC, HOIC, XOIC
DNS Amplification Attack	UDP	Spoofed	Very Large	High	Small (for request packet) Large (for response packet)	PyLoris, LOIC, HOIC, XOIC
NTP Amplification Attack	UDP	Spoofed	Large	High	Small (for request packet) Large (for response packet)	PyLoris, LOIC, HOIC, XOIC
ICMP Flood Attack	ICMP	Spoofed	Very Large	Very High	Variable	XOIC, Hping3, Hyenae
ICMP Fragmentation Attack	ICMP	Spoofed	Moderate	Very High	Large	XOIC, Hping3
Ping Flood Attack	ICMP	Spoofed	Very Large	Very High	Small	XOIC, Hping3, Hyenae

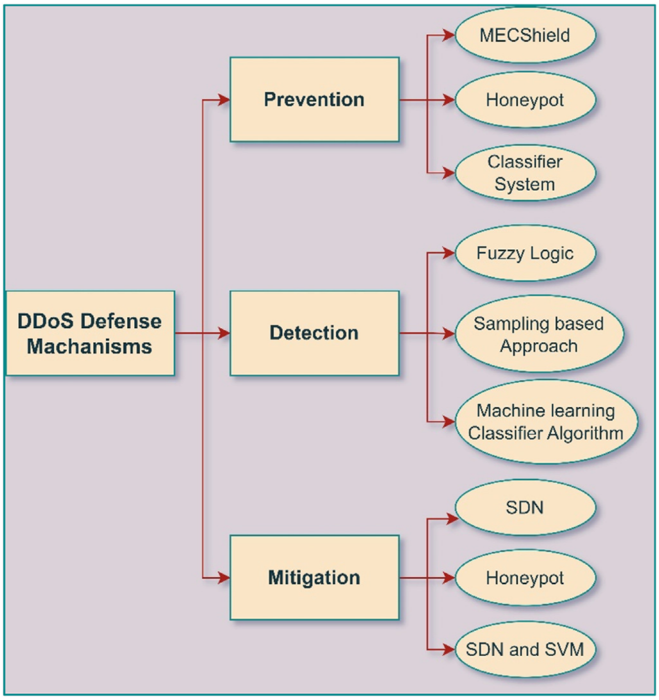

Fig. 14. Defense Mechanisms for mitigating DDoS Assault in IoT.

takeover, or disable the system/server. Various mechanisms can be implemented to prevent the attack. For example, Honeypot-based, Machine Leaning Classifier-based, Multi-access level edge computing Learning Automata-based (Misra et al., 2011), etc. DDoS attack detection is an essential part of performing mitigation methods over the network. Fig. 14 shows some important DDoS defense mechanisms.

For the detection of a DDoS attack, one needs to gather sufficient network traffic information and perform traffic analysis to figure out whether the traffic is legitimate or fraudulent (Cvitic´et al., 2021). As soon as the attacked system could be able to detect the attack, it would be able to perform mitigation on the attack (Agrawal and Tapaswi, 2019). Hence, each detection mechanism should have two key features to successfully detect the attack. One is the speed of attack detection and accuracy of attack detection. DDoS attack detection techniques can be widely categorized into two types based on the type of detection. In-line attack detection and Out-of-band attack detection (Li et al., 2021; Kentik, 2021). In-line attack detection means, through examination of incoming packets. Dedicated appliances are needed for deep packet inspection. But when the attacks are high in volume, these in-line detection appliances could be overwhelming hence Out-of-band means of attack detection are needed. Out-of-band work on traffic flow analysis. It receives the flow data from network devices like routers, switches, etc., and analyzes them to find out malicious activity (Kentik, 2021).

Mitigation of a DDoS attack is the last step of defense when prevention fails, and the victim has successfully detected the DDoS attack. Mitigation depends on lots of features of the network. For example, available bandwidth feature, an attack could hit the server if it exceeds the available bandwidth. Other such features are the deployment model, processing capacity, Routing techniques used, etc. (Doshi et al., 2021).

Many researchers have come across different DDoS defense methodologies; Some of them are described in Table 5:

Some of the DDoS attack defense mechanisms are explained in detail in the following subsections.

7.1. Honeypot-based defense mechanism

Honeypots are decoy computer systems that imitate the primary system in attracting potential cybercriminals seeking illegal access to the information system (Vishwakarma and Jain, 2019). Honeypot also helps to identify the method of attack by analyzing and gathering the information of the attack, such as the method of attack, the intensity of the attack, etc.

There are two types of honeypots categorized based on the interaction level with the attacker, Low interaction honeypots and High interaction honeypots. Honeypots can also be classified based on their requirements. Honeypots are used for research purposes and analyses of possible threats to the system or other shortcom-

Table 5
Systematic Analysis of Recent DDoS Defense Methodologies.

Research Work	Dataset Used	Description	Limitations
Filho et al. (2019)	• CIC-DOS • CICIDS2017 • CSE-CIC-IDS2018	Filho, et al. have proposed a machine learning-based approach for detecting DoS/DDoS attacks. The proposed system can detect both low and high-volume DDoS Attacks.	The approach works only on volumetric attacks and can be further extended to the analysis of vulnerabilities-based DDoS Assaults such as brute force.
Ravi and Shalinie (2020)	• UNB-ISCX	The researchers have proposed a novel approach for DDoS detection which is the Learning-Driven Detection Mechanism (LEDEM). It detects DDoS attacks using a supervised machine learning algorithm. LEDEM uses a decentralized cloud-SDN architecture.	The method is best suited for Trained/known attacks and not for Unknown or Untrained DDoS attempts.
Al-Duwairi et al. (2020)	_	The paper provides a SIEM (Security Information and Event Management) based Botnet detection approach which is used for the detection of volumetric DDoS assaults. The paper also highlighted some IoT network vulnerability detection methods such as Graph-based, Fuzzy based, and Network traffic pattern-based along with some other IoT botnet detection methods such as Anomaly-based, Signature-based, and Specification-based approaches.	The proposed approach only detects the attacks generated by bots but does not notice the attempts like Zero-day.
Doshi et al. (2021)	• N-BaIoT	Doshi, et al. have proposed an Online Discrepancy Test ODIT- based IDS approach for DDoS detection and mitigation.	The paper mainly focuses on Stealthy and low-rate DDoS Attacks as well as real-time implementation the system should be updated intermittently.
Kumar et al. (2021)	• BoT-IoT dataset of UNSW Canberra Cyber (For Training) • Real-time traffic (For Testing)	The researchers have used Machine learning and Deep learning algorithms for analyzing the DoS/DDoS attacks. The proposed method classifies the attacking traffic as normal one.	The model uses much time for training purposes which in turn makes a delay while classifying the network traffic.
Li et al. (2021)	• NB15 from UNSW Canberra Cyber	Li, et al. proposed a DDoS mitigation approach for improving the accuracy and minimizing the mitigation response time and named it FLEAM (Federated Learning Empowered Architecture to Mitigate DDoS). The paper states that the proposed methodology lowers the Mitigation response time up to 72% on average. The researchers used the IMA-GRU (Iterative Model Averaging based Gated Recurrent Unit) protocol for detection.	The paper focuses on mitigation response time but lacks frequent peer-to-peer communication during the learning process.
Bhayo et al. (2021)	_	Bhayo, et al. have proposed a Software Defined Network (SDN) based security framework for detecting IoT vulnerabilities and Suspicious traffic. They used SDNWISE (Software Defined Network Wireless Sensor Network) for DDoS attack detection.	The proposed approach does not block the detected malicious nodes, only detects the DDoS Flooding attempts.
Sharma et al. (2021)	• DARPA99	A protocol-based DDoS attack anomaly detection model is proposed using the CRPS (Continuous Ranked Probability Score). It mainly focuses on the TCP-SYN and Smurf attacks.	The model only identifies the anomaly present in the data rather than identifying the hostile node.

ings in the system, these types of honeypots are called Research Honeypots. Production honeypots are used to protect the company's server from DDoS attacks in real time. The honeypot setup can be distinguished into two parts for the process of DDoS attack defense. The primary step is the detection of abnormalities in the received packet with the help of IDS, and if any such abnormal request is discovered, then it will be directed to the honeypot rather than the host system (Vishwakarma and Jain, 2020). The honeypot has all the information of the defendant (who may be an attacker, which contains IP address, MAC address), etc. All this information is stored in the database. These log files are then used for further detection of malicious activities. The client is asked to authenticate on the basis of data collected by the honeypot, and the authenticity is checked. If it is found to be spam, the client is blocked from the system. If the client successfully passes the authentication process, then the traffic is routed to the main server for the service as shown in Fig. 15.

Nowadays, this honeypot is often combined with machine learning for better detection of the attack. A classification model is created to classify between normal and attack traffic, and then the machine learning model is used in the honeypot at the primary stage to detect the attack.

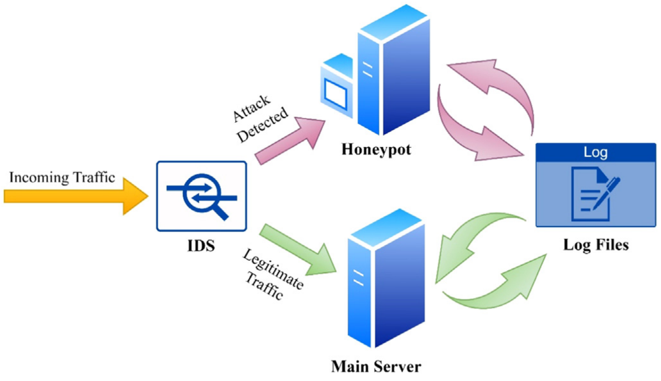

Fig. 15. Honeypot-based DDoS defense mechanism.

7.2. MECshield (Dao et al., 2021)

There is a mechanism called MECshield (Mobile Edge Computing) for the prevention of DDoS attacks. In this mechanism, some types of filters are used at the edge of the network to stop ma-

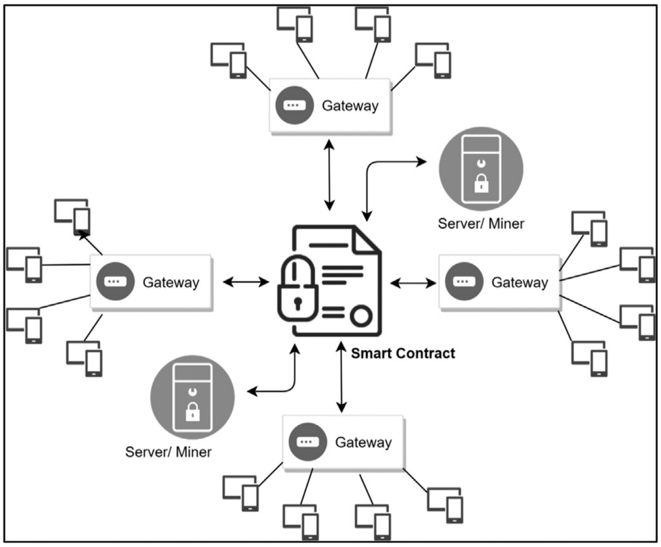

Fig. 16. Blockchain-Based DDoS Defense Architecture.

licious traffic from entering the system. There is a central controller that controls all the smart devices connected to it. The central controller actively communicates with all the filters to update the identifying features of the attack traffic. If the attack happens, the problem of the traffic bottleneck is dealt with by more than one smart filter at different edge points of the network. The central controller is trained with the traffic collected from all the smart devices. While training the smart filters, all important features required to detect attack traffic are used like port number, the number of packets, the protocol used, etc. The filters are required to place strategically for better detection of the attack. The three types of attacks that this mechanism can detect are sensor traffic, alarm traffic, and monitor traffic (Chen et al., 2022a, 2022b).

7.3. Blockchain-based method

A blockchain is an immutable and continuously growing chain of blocks in a distributed manner as shown in Fig. 16. Because of that, it is known as distributed ledger technology where blocks are made up of digital information like a hash of the previous block and timestamp (Noor and Hassan, 2019; Tiana et al., 2019). The blockchain uses cryptographic algorithms to provide security to the blocks. The technology uses math functions and other self-executable programs known as smart contracts (Silva et al., 2020). The security of a blockchain depends on the smart contract. The security for communication between distributed servers and IoT devices also depends on a smart contract. There are several smart contracts like Ethereum, Bitcoin, Pi, etc. which are some of the largest established online platforms. In addition to their state, this platform allows for building smart contracts and De-centralized applications (DApps). In Ethereum, a state is the data present in blocks, and a state transition takes place when a transaction occurs and each transaction is verified by the other nodes of the network. Ethereum has some sort of resource limit which is used as a threshold so that once the limit is exceeded, the system totally cut off every resource for further use. This limit prevents system overloading and is needed to be set for every transaction processed. This limit is set to prevent the network from being attacked. Since blockchain technology works on a decentralized approach, we can prevent an IoT network from single-point failure by implementing Ethereum over it. After deploying Ethereum with IoT the whole is termed an IoT-Ethereum network. The smart contract for this network maintains a list of authorized devices or nodes. So, when a device requests a service, the contract verifies it first from the list and then provides access to that. This methodology prevents the network from DDoS by limiting the resources. To execute a DDoS assault all the nodes of the network may start requesting the resources at the same time but the resource limit set by Ethereum block the services after hitting the maximum resource limit. The importance of blockchain here is its transparency and decentralized data storage, which makes it difficult for the attack (Javaid et al., 2018).

7.4. Machine learning-based methods

The Machine learning-based classification mechanism can also be used to prevent DDoS attacks in IoT networks. There are several classification algorithms that can be used to differentiate attack data and normal data (Bailey et al., 2007) and the selection of effective machine learning algorithms can be problematic. To solve that issue Shafiq et al. (2020) have proposed a selection procedure model by using the Bijective Soft Set approach. The Bijective soft set is a mathematical model which is used for concept selection and decision-making. Yuan et al. (2017) have used the Naive Bayes Classifier Multi-Agent Intrusion Detection System (NBC-MAIDS), in this detection mechanism agent, is used that is deployed across the nodes in the network and works as multi-agents. These agents are used to monitor the traffic and manage the nodes in the network. These multi-agents classify the incoming traffic data, whether it is attack traffic or legitimate traffic. If the traffic is malicious, then drop it or completely block it. After dropping the traffic, it manages the database and updates it with the latest information of the attack, and communicates with other agents to effectively block the malicious traffic and manage the attack detection and share information with each other. The higher detection rate in this mechanism is due to machine learning-based solutions and multi-agents (Alrehan and Alhaidari, 2019).

Another machine learning-based technique detected and prevented DDoS assaults on the IoT network by using the LS-SVM (Least Squares Support Vector Machine) classifier system (Hoyos Ll et al., 2016). The classifier analyses the incoming traffic and takes proper action according to the type of traffic. The mechanism has two phases, detection of attack and prevention of attack. In the detection phase, the system collects information on incoming traffic and verifies it with the prior formed database. If the incoming traffic contains information which is matching with the one in the database as malicious, it will directly prevent the flow from entering the IoT network. But if the traffic is normal then the model will send the traffic through the classifier to make sure the traffic is not malicious. (Bailey et al., 2007).

7.5. Image processing-based method

It is a simple lightweight method for detecting IoT malware that uses malware picture categorization. The principle of image processing is used to identify various malware behaviors and then evaluate them. The use of image processing could be useful because of the fact that IoT malware behaves rather differently from standard malware because it attempts to destroy other malware to capture enough computer resources. The basic need for converting malware code to pictures is to get the CNN input vectors, which are 8-bit vectors. It just takes a rearrangement of the malware programs (without any further pre-processing of the real image). To maintain balance in CNN, all pictures for input are rescaled to 64 × 64 pixels. The configuration used is a light weighted, two-layer Convolutional Neural Network as shown in Fig. 17. Due to the processing power, this mechanism is faster as compared to the conventional signature-matching method for detection (Rieck et al., 2008). Due to its feature extraction by using deep learning, CNN

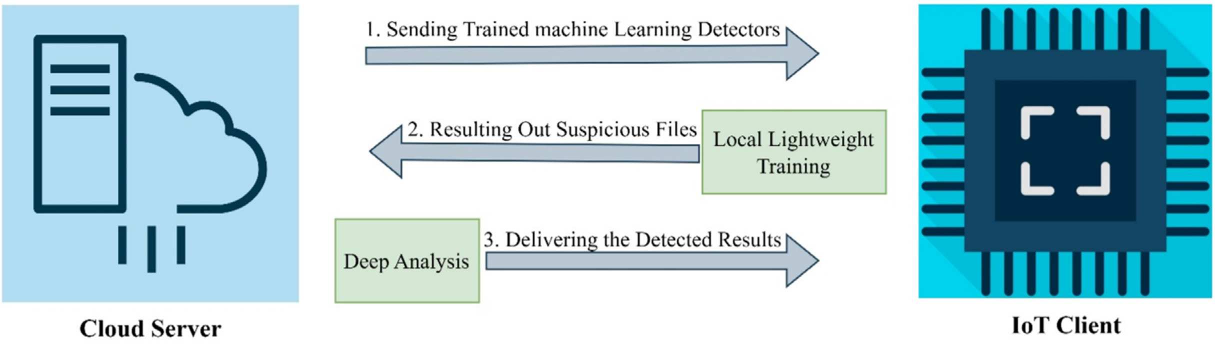
1. Sending Trained machine Learning Detectors
2. Resulting Out Suspicious Files
Local Lightweight Training
Deep Analysis
3. Delivering the Detected Results
Cloud Server
IoT Client

Fig. 17. A lightweight malware detection model.

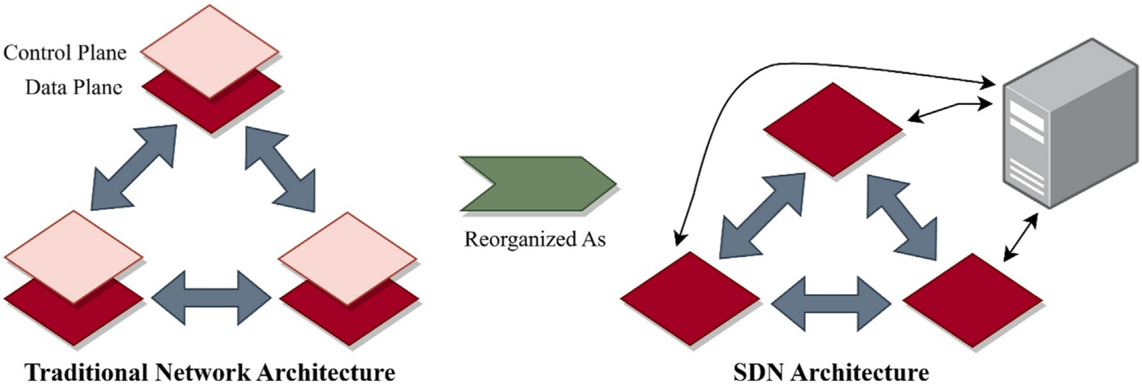

Fig. 18. Traditional vs SDN-Based Network Architecture.

has emerged as a stronger and more powerful classifier among other types of classifiers and has a better test stage performance (Yuan et al., 2017).

7.6. Machine learning with SDN based

The method uses Machine learning for classification purposes and Software Defined Networks (SDN) for the detection of attack traffic (Dayal et al., 2016). The SDN uses an SDN controller as shown in Fig. 18 which is used to consistently track the traffic flow of packets and report network anomalies detected using the SDN controller (Li et al., 2020; Gong et al., 2019). For classification of the malicious packet flow, a Support Vector Machine (SVM) is added to the controller. When the source malicious traffic is detected with the help of an SDN controller, it is blocked. The SDN controller is then updated so that it can prevent the attacking machine from interacting with other systems or nodes by using the newly defined attack (Kotey et al., 2019). With TCP flooding attacks, the suggested solution is verified. The mechanism uses Mininet to mimic the functionality of IoT gadgets and utilizes numerous attacking approaches to evaluate the mechanism (Bhunia and Gurusamy, 2017; Ubale and Jain, 2018).

SDN architecture has been used to offer several sorts of DDoS attack mitigation mechanisms such that:

(a) In terms of packet flow, controllers can be used for network attacks to regulate the entire SDN network universally. Any divergence from the usual behavior in the network traffic can be easily identified by the controller and enforced by preemptive action to avoid the outbreak (Brajones et al., 2020).
(b) For a Source-based attack, if an attack relies on a network anomaly, controllers might be used to recognize it, then alter the packet information at the network edge (Silva et al., 2020).
(c) In order to identify and prevent cross-domain threats from geographically dispersed IoT devices, SDN infrastructure operates in parallel with a standard IP network to share information, forward traffic, and other collective tasks (Dayal et al., 2016).

7.7. Middleware based

This defense mechanism is developed specifically for IoT users. One of the key components of the design is a cross-domain middleware called Networked Smart Object (NOS). Fig. 19 depicts the NOS architecture. In an IoT ecosystem, Internet of Things (IoT) devices are responsible for collecting the open information stream in real time. There are IoT nodes such as RFID (Radio Frequency Identification), NFC (Near Field Communication), actuators, etc. in its infrastructure. The Message Queue Telemetry Transport (MQTT) protocol provides authentication-based flexible and secure sharing of information. The entire process under NOS is controlled by the enhancement system to make sure the correct and proper implementation of developed policies. Interaction between the NOS components occurs through a freely accessible RESTful interface. While numerous ad hoc solutions have been proposed for traditional networks such as WSN and MANETs, however, this approach is particularly offered for the IoT platform and its services. The overall infrastructure is made up of numerous NOSs distributed in a large area which makes it easy to link the data situated at heterogeneous places to the neighboring NOSs. The transmission of data to the NOS, for a source, is done through a public channel. To allow data connectivity using HTTP for communication, each public port is comprised of NOS.

In turn, the NOS will verify the source, and only with a strong response obtained from the NOS, the source will be able to supply its information in encrypted form. To avoid unnecessary wasting of resources during a DDoS attempt, one can generate several dynamic ports on each NOS based on the number of connec-

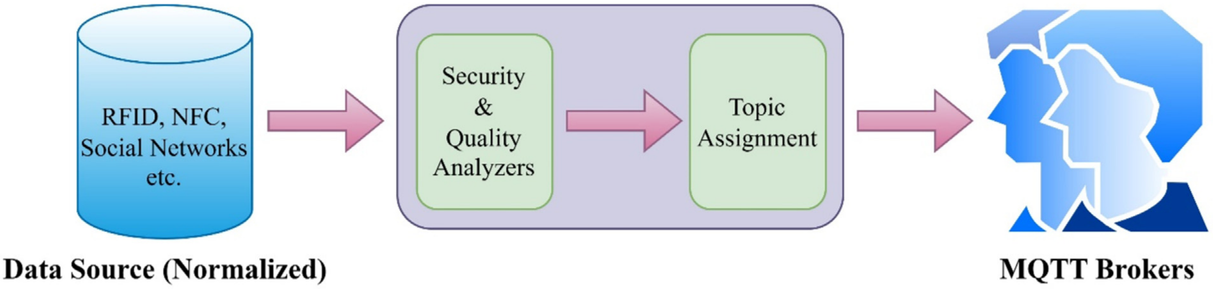

Fig. 19. NOS Architecture.

tions. These virtual ports serve to switch between the connected users' sets. A unique identifier is created and randomly allocated to each NOS by Overload Balance Manager (OBM). Using a secure VPN, Overload Balance Manager acts as a virtual machine that is connected to all the NOS in the Internet of Things network. This Unique Identifier, when connected to the virtual port of the network, forms a unique address that is way too difficult to hack by attackers (Sicari et al., 2018).

Every NOS can respond to the following cases of seeking a DDoS attack on IoT.

(a) **Case 1:** Sudden Increase in the received packets numeral: when the NOS port receives packets from the same port or the same, then it will be rejected for a given threshold. In this way, the excessive analysis and processing of irrelevant information are avoided.
(b) **Case 2:** Increase in the number of connection requests: NOS rejects the link requests by tossing an exception about the unavailability of its resource when the incoming requests for the connection exceed the dynamically determined threshold value.
(c) **Case 3:** When UID is known to Malicious entity: If a perpetrator has somehow known about only one of the UID of multiple ports, then the system becomes quite vulnerable because it is possible to detect an active virtual port by simply using the brute force approach as it is only a serial number corresponds to the known UID. When this case happens, the potentially targeted NOS is placed in a new location given by OBM with an updated UID and then the same NOS starts a new instance that was relocated.
(d) **Case 4:** When the address is known to a malicious entity: If any sources keep flooding the channel unnecessarily with illegitimate frame segments on the established ports of NOS even after NOS drops and close the session, all the operational connections on that specific channel will be eradicated forcefully, and the port will be renamed by assigning a new port number to it.
(e) **Case 5:** When resources are still consumed by compromised sources: The solution of the previous case is expanded here. When the OBM detects some kind of suspicious operation, that particular NOS is disabled and shifted to some other place, and a new instance is initiated, isolating the particular compromised NOS from the IoT network so that the attack does not evolve. Besides these countermeasures, the infected sources have the capacity to drain the resources of the network such as the bandwidth of the network, Processing power, and memory.

7.8. Hybrid defense approaches

Along with the mentioned methodologies, researchers also merge two or more methods and develop a hybrid approach to get better results. We have gone through the mentioned hybrid methodologies:

(a) **Hybrid IDPS** (Shurman et al., 2020)**:** Intrusion Detection and Prevention system utilizes two methodologies which are the Signature-based and Anomaly-based methods for detection purposes. Shurman, M. et al. (2020) have proposed a hybrid approach by combining both of these techniques. The signature-based method detects the attack by observing the attack signatures, malicious code sequences, and weird patterns while the anomaly-based technique analyzes the network traffic and compares its behavior with the previous normal network traffic behavior. In the hybrid approach if one of the techniques is unable to detect a particular attack, then the other will detect it. That is how the hybrid approach provides more accurate detection of the attack.
(b) **Deep Learning-Driven SDN-based Hybrid Mechanism** (Javeed et al., 2021)**:** Javeed, D. et al. (2021) have proposed a hybrid defense methodology by enabling the SDN with a Deep Learning-Driven framework. Since IoT works in a heterogeneous environment and the SDN enhances the dynamicity of IoT as well as it also simplifies the network management of IoT, because it uses an SDN controller to manage and analyze the network traffic. To make the detection more effective the researchers have used Cuda-deep neural network, gated recurrent unit (Cu- DNNGRU), and Cuda-bidirectional long short-term memory (Cu-BLSTM) and developed the hybrid model. This hybrid model is then deployed over the control plane of SDN enabled IoT network. The technique can detect the attacks like DDoS, infiltration, and brute force attacks.

There can be other defense methodologies present to defend against the DDoS attack or to minimize its effect. Yu, et al. (2021) have proposed a semisupervised machine learning model by combining the Random Forest and Spectral Clustering techniques to detect another variant of DDoS which is the WebDDoS attack (Yu et al., 2021). Several hybrid approaches can also be developed by merging two or more techniques to get a better result and to create a robust mechanism. However, most of the methods are not platform-independent and it is hard to deploy them over the framework where the minimum requirements for the model are not satisfied. To discover the relevant one, we have compared these mechanisms in the next section by writing some of the advantages and vulnerabilities they carry with them.

7.9. Comparative analysis of existing DDoS defense mechanisms

We have gone through all of the defensive mechanisms in the previous section and to get an optimal defense mechanism for DDoS attacks on IoT we need to analyze these mechanisms completely. Table 6 presents some of the defense mechanisms with their proposed model, important points that the mecha-

Table 6
Comparative analysis of existing DDoS defense mechanisms.

Defense Mechanism	Model	Key points	Vulnerabilities
Honeypot-based defense (Vishwakarma and Jain, 2020)	A decoy system is used parallel along with the Intrusion Detection System to redirect the attack traffic.	• Attack traffic gets redirected to the honeypot when the potential of attack increases, instead of being directly received by the main server. • Any unknown malware detected by the honeypot can be used for actively understanding the details of the attack and the honeypot would be able to detect such attacks in the future.	• The mentioned system cannot be incorporated in a real-time setting; however, it can be implemented utilizing a central server with a microcontroller interface. • It is not capable to handle volumetric attacks, which use large botnets
Mobile Edge Computing-based defense (Dao et al., 2021)	Filters are used at the edge of the network for the detection of DDoS attacks.	• A central controller that controls all the smart filters. • The filters are self-improving and use self-organizing map filters to train separately	• The central controller may get attacked, which results in the failure of defense.
Blockchain-based Defense (Javaid et al., 2018)	Blockchain uses a smart contract, which is a self-executable program.	Blocks in this mechanism are considered to be an uncompromised devices in any situation.	Unrealistic assumption of gateway being uncompromised during DDoS attack. It is not capable to handle advanced botnet attacks.
SDN-based Defense (Bhunia and Gurusamy, 2017)	SDNi extension is used to deal the DDoS attacks in multiple SDN domains.	• Restricts the attack from hitting the network firewalls or any other monitoring mechanisms by isolating the attacked device and reconfiguring it. • Minimizes congestion problems and prevents the attack from being exacerbated by malicious IoT devices.	• Possess a security threat because of its centralized control mechanism. • May not be able to detect newer types of attacks.
Middleware-based Defense mechanism (Sicari et al., 2018)	A Networked Smart Object is used at the edge of the network.	• NOS can receive data in real time and filter this data to detect DDoS attacks from remote and heterogeneous IoT devices. • Message Queue Telemetry Transport (MQTT) protocol is utilized to authenticate, publish and subscribe mechanisms for exchanging lightweight and secure information.	• The mechanism is not scalable, the volume of attacks it can handle depends on the number of NOS. • As the protocol used works over TCP, it requires a large number of resources for the power and memory of the mechanism.
Machine learning-based defense mechanisms (Bailey et al., 2007)	Supervised and unsupervised learning models, as well as a neural network, are used.	• Able to detect attacks with fewer false positives/negatives. • Able to detect both traditional and IoT-based DDoS attacks with the help of various classification algorithms.	• The reliability of a dataset used to train the system for detecting DDoS attacks in IoT is directly related to its accuracy.
Hybrid IDPS (Shurman et al., 2020)	Intrusion Detection Prevention system is used by combining both the Signature-based and Anomaly-based detection methodologies.	• The approach is able to detect unknown attacks and DoS attacks by analyzing the network behavior and attack signature patterns. • The approach shows a faster detection rate after integrating the methodologies.	• The method generally detects DoS attacks and is less relevant for DDoS attack detection. • The anomaly-based detection methodology sometimes produces a higher False Positive rate.
Deep Learning-Driven SDN-based Hybrid Mechanism (Javeed et al., 2021)	The researchers have applied Deep Learning models over the SDN-enabled IoT network.	• The SDN controller tracks the network traffic and reports the network irregularities. • The deep learning models which are employed over the control plane are able to detect DDoS and infiltration attacks effectively	• The hybridization makes the model more complex to deploy over a huge network. • Also, the accuracy of the model depends on the reliability of the dataset which is used to train and test the Deep Learning models.

Table 7
Defense mechanisms for various DDoS Attacks.

DDoS Attacks	Methods
Protocol Exploitation Attacks	• Machine Learning and Deep Learning models • SDN-based defense techniques • Mobile Edge Computing
Forged Packet Attack	• Image Processing Based • Mobile Edge Computing • Machine Learning and Deep Learning models • SDN-based defense techniques
Amplification Attacks	• Machine Learning and Deep Learning models • Hybrid Models using SDN and Classifier models • Mobile Edge Computing
Zero-Day Attack	• Hybrid IDPS • Honeypot-based methodology along with signature/anomaly-based detection (Innab et al., 2018)
Infrastructure Attack	• SDN-based defense techniques • Image Processing Based

nism address, and the vulnerabilities of the model. Most conventional approaches are not capable of adequately detecting and mitigating DDoS attacks on the application layer, however, in that case, a machine learning mechanism can actively detect such attacks because of its effective and lightweight classification algorithms.

We have analyzed the defense methodologies and listed their comparisons in this section. We have presented the main advantages and disadvantages of each method in Table 6. Honeypot-based methodology redirects the attack traffic while mobile edge computing and SDN-based mechanisms use a controller to filter the malicious traffic. The researchers are using machine learning algorithms widely for detecting the attacks but it relies on the quantity and quality of datasets used to train the models. However, detecting the relevant approach is still a question for users. Hence, we have listed the possible solutions to mitigate the different types of DDoS attacks in Table 7.

Since each method faces some vulnerabilities hence, one should implement some preventive measures while working with IoT, the next section lists some of them.

8. Preventive measures to mitigate DDoS attacks

The fact is that there is no single solution that will protect you completely from DDoS attacks. By adopting the following measures, an organization may greatly decrease the chance of a DDoS assault occurring and the damage if an attack does take place (Robinson, 2021; Maria, 2020).

8.1. Upgrading the network security infrastructure

There are several components that make up an effective security system, including the moment when you replace your network infrastructure if it's outdated and inefficient. As a first step, you should boost your bandwidth. DDoS assaults create rapid increases in traffic, and this allows networks and servers to handle them. It is also necessary to implement multi-layered network security. Hence, data centers should not be centrally located, and infrastructure components should be placed at distinct locations. So that, if one region is attacked, the rest of the system can continue to function normally (Robinson, 2021).

8.2. Switching to cloud schemes

To increase flexibility and resilience in their IT operations, organizations have been moving from on-premises systems to cloud-based ones over the last few years. These solutions are more secure because they use industry best practices and feature up-to-date patching. As far as preventing DDoS attacks is concerned, cloud-based systems have taken the decentralization method way beyond imagination. If companies want the most flexible DDoS protection, they should explore a multi-cloud strategy with several cloud providers or a hybrid solution that uses both off-premises and on-premises technologies (Maria, 2020).

8.3. Detect traffic anomalies with network monitoring and DDoS mitigation tools

It is important for small companies to check their bandwidth and be on the lookout for traffic fluctuations that might recognize a DDoS attempt. First-level security is provided by network monitoring tools, which monitor traffic and warn you when there is an abnormal increase in the packet rate. Both of these technologies, in conjunction with DDoS mitigation solutions, aid in the detection and mitigation of DDoS attempts. You may detect security problems on your network by analyzing your network logs, using Web application firewalls, load balancers, and other network protection technologies that are also available (Maria, 2020).

8.4. Develop a DDoS mitigation action plan before it's too late

Even if you apply all of these security measures, mistakes can still occur despite your efforts. Having a DDoS mitigation plan in place is the best way to protect your server in the event of a DDoS assault. As part of their data protection strategy, companies should put together a DDoS response team that is technically skilled, and to do this, the team should develop a number of different techniques for identifying and mitigating. Depending on how essential a server is, different techniques may be required. DDoS attacks can cripple a firm if it does not have a comprehensive recovery strategy that includes several malfunctions (Robinson, 2021).

8.5. Adopting better network security practices

Cybercriminals can exploit any loopholes in your security measures, which is why they should be impenetrable. For instance, the default passwords on many IoT devices are weak. For this reason and the fact that their numbers are continuously increasing, they are ideal targets for hackers wanting to extend their botnet. IT professionals should adopt multi-factor authentication techniques and update all passwords regularly to avoid mistakes. A firm with a large number of employees and a high turnover rate would also benefit from compartmentalization and access controls. Your most valuable resources and information do not have to be accessible to everyone, and limiting access can help prevent DDoS attacks on these components (Robinson, 2021).

9. Challenges and open research issues

Defending IoT networks from DDoS attacks is an evolving research field with the growth of smart devices. Although, many researchers have given several defense mechanisms including detection methods and prevention methods. But there are some challenges and issues present which are still open such as:

- There is no standard architecture available for IoT. There are many layered models present for IoT but not a single standardized framework is available which creates a loophole because the defense methods are developed using different frameworks and some of them are not platform-independent.
- Many machine learning-based defense methodologies depend on the training datasets to train the model. These models use DDoS flooding data for training purposes which is not reliable for real-time traffic because the assurance of same quality traffic data is quite problematic.
- Small IoT devices are not capable enough for smart data management including data collection and extraction and to handle that some security administrators connect these devices to one high computational device which may lead to single-point failure if attacked by the attacker.
- The defense methodologies are not smart enough to combat slow network distortion caused by DDoS attacks as attackers are evolving their DDoS attempt procedures and a majority of the defense methods focus on quick network destruction.
- The development of DDoS defense methodologies should consider the balance of hardware and software used in IoT and network flexibility so that the QoS (Quality of Service) can be maintained.
- Other than this some other open issues can be the inability to detect or prevent unknown attacks like zero-day DDoS attacks and unable to implement most of the defense methods in a real-time scenario.

10. Conclusion and future work

Undeniably, IoT is having an evolving era as the technology is growing uninterruptedly and IoT is connecting devices as well as humans. With this rapid growth of technology, the IoT is becoming more vulnerable and the center of attraction for hackers. Attackers exploit the network to gain access to it. Among a variety of attacks, a DDoS attack behaves contrarily as it does not reveal any signs of device failure and is hence hard to avoid. A detailed and rigorous examination of DDoS assaults is given in this survey. In this survey, firstly, we have presented the statistics of some infamous DDoS attacks followed by the motivations for deploying the attack. Later, we compiled a list of the many sorts of assaults we have observed so far and the numerous ways that are used to perform the assault. The paper also covers the architecture of DDoS attacks and the botnet command and control model. An intruder uses this command-and-control architecture to persuade an assault by commanding the bot devices. There are many botnets present in the market which are used by attackers. We have listed a few of them providing a brief explanation of their use and harmfulness. Further, we have noted the most important characteristics of the defense mechanisms which are used to overcome the threat of attack by detecting, preventing, and defending with their advantages and disadvantages. There can be other defense mechanisms also available to minimize the effect of DDoS and to procure it. However, machine learning and SDN-based methodologies are widely used nowadays. Lastly, the paper discusses some basic prevention measures to avoid the attack. This survey will give a simple basis for understanding DDoS assaults, as well as a structured explanation and interpretation. Since the researchers have provided a variety of solutions to defend against DDoS attacks. However, these solutions should be more intelligent and smarter to combat the new variants of DDoS attacks and attacking methods.

Declaration of Competing Interest

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

Data Availability

No data was used for the research described in the article.

References

Aamir, M., Zaidi, M.A., 2013. A survey on DDoS attack and defense strategies: from traditional schemes to current techniques. Interdiscip. Inf. Sci. 19 (2), 173–200.

Afek, Y., Barr, A.B., Cohen, E., Feibish S.L., Shagam, M., "Efficient distinct heavy hitters for DNS DDoS attack detection," arXiv:1612.02636v1, pp. 1–9, December 2016, https://doi.org/10.48550/arXiv.1612.02636.

Agrawal, N., Tapaswi, S., 2019. Defense mechanisms against DDoS attacks in a cloud computing environment: state-of-the-art and research challenges. IEEE Commun. Surv. Tutor. 21 (4), 3769–3795.

Akram, H., Ghani, A., Konstantas, D., Mahyoub, M., 2018. A comprehensive IoT attacks survey based on a building-blocked reference model. Int. J. Adv. Comput. Sci. Appl. 9 (3), 355–373.

Al-Duwairi, B., Al-Kahla, W., AlRefai, M.A., Abdelqader, Y., Rawash, A., Fahmawi, R., 2020. SIEM-based detection and mitigation of IoT-botnet DDoS attacks. Int. J. Electr. Comput. Eng. (IJECE) 10 (2), 2182–2191.

A. G. M. M. M. A. M. & Al-Fuqaha, A.M., 2015. Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutor. 17 (4), 2347–2376.

Alrawais, A., Alhothaily, A., Hu, C., Cheng, X., 2017. Fog computing for the internet of things: security and privacy issues. IEEE Internet Comput. 21 (2), 34–42.

Alrehan, A.M., Alhaidari, F.A., 2019. Machine learning techniques to detect DDoS attacks on VANET system: a survey. In: Proceedings of the 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, pp. 1–6.

Anand, P., Singh, Y., Selwal, A., Singh, P.K., Felseghi, R.A., Raboaca, M.S., 2020. IoVT: internet of vulnerable things? Threat architecture, attack surfaces, and vulnerabilities in internet of things and its applications towards smart grids. Energies 13 (4813), 1–23 September.

Anirudh, M., Thileeban, S.A., Nallathambi, D.J., 2017. Use of honeypots for mitigating DoS attacks targeted on IoT networks. In: Proceedings of the International Conference on Computer, Communication and Signal Processing (ICCCSP). Chennai, India.

Atzori, L., Iera, A., Morabito, G., 2010. The Internet of Things: a survey. Comput. Netw. 54 (15), 2787–2805 28 October.

Bailey, M., Oberheide, J., Andersen, J., Mao, Z.M., Jahanian, F., Nazario, J., 2007. Automated classification and analysis of internet malware. In: Proceedings of the International Workshop on Recent Advances in Intrusion Detection, 4637, Berlin, Heidelberg, pp. 178–197.

Behal, S., Kumar, K., 2017. Detection of DDoS attacks and flash events using information theory metrics–an empirical investigation. Comput. Commun. 103, 18–28 1 May.

Bhayo, J., Jafaq, R., Ahmed, A., Hameed, S., Shah, S.A., 2021. A time-efficient approach towards DDoS attack detection in IoT network using SDN. IEEE Internet Things J. 1–20 April.

Bhunia, S.S., Gurusamy, M., 2017. Dynamic attack detection and mitigation in IoT using SDN. In: Proceedigns of the 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, pp. 1–6.

Bhuyan, M.H., Bhattacharyya, D.K., Kalita, J.K., 2015. An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. Pattern Recognit. Lett. 51, 1–7 January.

Brajones, J.G., Murill, J.C., Valdés, J.F.V., Valero, F.L., 2020. Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: an experimental approach. Sensors 20 (816), 1–19 Febraury.

Britannica, T.E.o.E., "Syrian-Civil-War," 17 July 2020. [Online]. Available: https://www.britannica.com/event/Syrian-Civil-War. [Accessed 10 June 2021].

Celeda, P., Krejci, R., Vykopal, J., Drašar, M., 2010. Embedded malware - an analysis of the chuck norris botnet. In: Proceedings of the 6th European Conference on Computer Network Defense – EC2ND, Berlin, Germany, pp. 3–10.

Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., Jin, Y., 2018. Internet-of-things security and vulnerabilities: taxonomy, challenges, and practice. J. Hardw. Syst. Secur. 2 (2), 97–110 may.

Chen, M., Liu, W., Zhang, N., Li, J., Ren, Y., Yi, M., Liu, A., 2022a. GPDS: a multi-agent deep reinforcement learning game for anti-jamming secure computing in MEC network. Expert Syst. Appl. 210 (118394), 1–16 20 December.

Chen, M., Liu, W., Wang, T., Zhang, S., Liu, A., 2022b. A game-based deep reinforcement learning approach for energy-efficient computation in MEC systems. Knowl. Based Syst. 235 (107660), 1–14 10 January.

Chickowski, E., "Types of DDoS attacks explained," 8 July 2020. [Online]. Available: https://cybersecurity.att.com/blogs/security-essentials/types-of-ddos-attacks-explained. [Accessed June 2021].

Cirillo, M., Mauro, M.D., Matta, V., Tambasco, M., 2021. Application-layer DDOS attacks with multiple emulation dictionaries. In: Proceedings of the ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Toronto, ON, Canada.

Crane, C., "The 15 top DDoS statistics you should know in 2020," 16 November 2019. [Online]. Available: https://cybersecurityventures.com/the-15-top-ddos-statistics-you-should-know-in-2020. [Accessed May 2021].

Crane, C., "*Re*-hash: the largest DDoS attacks in history," 25 June 2020. [Online]. Available: https://www.thesslstore.com/blog/largest-ddos-attack-in-history. [Accessed March 2021].

Cvitić, I., Perakovic, D., Perisˇa, M., Botica, M., 2021. Novel approach for detection of IoT generated DDoS traffic. Wirel. Netw. 27 (3), 1573–1586.

Czyz, J., Kallitsis, M., Gharaibeh, M., Papadopoulos, C., Bailey, M., Karir, M., 2014. Taming the 800 Pound Gorilla: the rise and decline of NTP DDoS attacks. In: Proceedings of the Conference on Internet Measurement Conference (IMC '14), New York, USA, pp. 435–448.

Dao, N.N., Phan, T.V., Sa'ad, U., Kim, J., Bauschert, T., Do, D.T., Cho, S., 2021. Securing heterogeneous IoT with intelligent DDoS attack behavior learning. IEEE Syst. J. 1–10 June.

Dayal, N., Maity, P., Srivastava, S., Khondoker, R., 2016. Research trends in security and DDoS in SDN. Secur. Commun. Netw. 9 (18), 6386–6411.

Devdiscourse, "Google absorbed record-breaking 2.5 Tbps DDoS attack in September 2017," 17 October 2020. [Online]. Available: https://www.devdiscourse.com/article/technology/1264631-google-absorbed-record-breaking-25-tbps-ddos-attack-in-september-2017. [Accessed 2021].

Devine, S.M., 2016. DDoS goes mainstream: how headline-grabbing attacks could make this threat an organisation's biggest nightmare. Netw. Secur. 2016 (11), 7–13 november.

Donno, M.D., Dragoni, N., Giaretta, A., Spognardi, A., 2017. Analysis of DDoS-capable IoT malwares. In: Proceedings of the Federated Conference on Computer Science and Information Systems, 11, PRAGUE, pp. 807–816.

Doshi, K., Yilmaz, Y., Uludag, S., 2021. Timely detection and mitigation of stealthy DDoS attacks via IoT networks. IEEE Trans. Dependable Secure Comput. 18 (5), 2164–2176.

Durfina, L., Kroustek, J., Zemek, P., 2013. PsybOt malware: a step-by-step decompilation case study. In: Proceedings of the 20th Working Conference on Reverse Engineering (WCRE), Koblenz, Germany, pp. 449–456.

Elleithy, K.M., Blagovic, D., Cheng, W.K., Sideleau, P., 2005. Denial of service attack techniques: analysis, implementation and comparison. J. Syst. Cybern. Inform. 3 (1), 66–71.

Farooq, M.U., Waseem, M., Khairi, A., Mazhar, S., 2015. A critical analysis on the security concerns of Internet of Things (IoT). Int. J. Comput. Appl. 111 (7), 1–6.

Ferrisbuller, "16 best DDOS attack tools in 2022," 23 January 2022. [Online]. Available: https://www.securityboulevard.com/2022/01/16-best-ddos-attack-tools-in-2022/. [Accessed 30 March 2022].

Filho, F.S.d.L., Silveira, F.A.F., Junior, A.d.M.B., Vargas-Solar, G., Silveira, L.F., 2019. Smart detection: an online approach for DoS/DDoS attack detection using machine learning. Secur. Commun. Netw. 2019, 1–15 October.

Frolova, V., "8 Biggest DDoS attacks in history," 5 December 2021. [Online]. Available: https://news.cheapdeveloper.com/webmaster/articles/1517-8-biggest-ddos-attacks-in-history.html. [Accessed 28 March 2022].

Gantz, J., Reinsel, D., 2012. "The digital universe in 2020: big data, bigger digital shadows, and biggest growth in the far east," IDC iView: IDC Analyze the future, vol. 2007, pp. 1–16.

Ghali, A.A., Ahmad, R., Alhussian, H.S.A., 2020. Comparative analysis of DoS and DDoS attacks in internet of things environment. In: Proceedings of the Computer Science On-line Conference CSOC 2020: Artificial Intelligence and Bioinspired Computational Methods.

Gong, C., Yu, D., Zhao, L., Li, X., Li, X., 2019. An intelligent trust model for hybrid DDoS detection in software defined networks. Concurr. Comput. Pract. Exp. 32 (2), 1–16 May.

Greenberg, A., "The reaper IoT botnet has already infected a million networks," 20 October 2017. [Online]. Available: https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/. [Accessed May 2021].

Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M., 2013. Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. 29 (7), 1645–1660 September.

Gupta, B.B., Joshi, R.C., Misra, M., 2009. Defending against distributed denial of service attacks: issues and challenges. Inf. Secur. J.: Glob. Perspect. 18 (5), 224–247.

Gutnikov, A., Kupreev, O., Badovskaya, E., "DDoS attacks in Q1 2021," 10 May 2021. [Online]. Available: https://securelist.com/ddos-attacks-in-q1-2021/102166/. [Accessed June 2021].

Hadhrami, Y.A., Hussain, F.K., 2021. DDoS attacks in IoT networks: a comprehensive systematic literature review. World Wide Web 24, 971–1001 January.

Hamza, Arshad, M., October 2019. Evaluating security threats for each layers of IoT system. International Journal of Recent Contributions from Engineering, Science & IT 10, 20–28. https://doi.org/10.3991/ijes.v10i02.29301.

Hern, A., "Google suffers global outage with Gmail, YouTube and majority of services affected," 14 December 2020. [Online]. Available: https://www.theguardian.com/technology/2020/dec/14/google-suffers-worldwide-outage-with-gmail-youtube-and-other-services-down. [Accessed 01 April 2022].

Hoyos Ll, M.S., Isaza, G., Velez, J., Castillo, L.F., 2016. Distributed denial of service (DDoS) attacks detection using machine learning prototype. Adv. Intell. Syst. Comput. 474, 33–41 January.

Innab, N., Alomairy, E., Alsheddi, L., 2018. Hybrid system between anomaly based detection system and honeypot to detect zero day attack. In: Proceedigns of the 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Saudi Arabia, pp. 1–5.

Intezer, "2020 set a record for new linux malware families," 24 February 2021. [Online]. Available: https://www.intezer.com/blog/cloud-security/2020-set-record-for-new-linux-malware-families/. [Accessed 31 March 2022].

Irum, A., Khan, M.A., Noor, Amna, Shabir, B., 2020. DDoS detection and prevention in internet of things. EasyChair (2486) 1–7.

Javaid, U., Siang, A.K., Aman, M.N., Sikdar, B., 2018. Mitigating loT device based DDoS attacks using blockchain. In: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, pp. 71–76.

Javapipe, "35 Types of DDoS Attacks Explained," 2016. [Online]. Available: https://javapipe.com/blog/ddos-types/. [Accessed 2021].

Javeed, D., Gao, T., Khan, M.T., Ahmad, I., 2021. A hybrid deep learning-driven SDN enabled mechanism for secure communication in internet of things (IoT). Sensors 21 (4884), 1–18 July.

Jerkins, J.A., 2017. Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code. In: Proceedings of the IEEE 7th Annual Computing and Communication Workshop and Conference, Las Vegas, NV, USA, pp. 1–5.

Jia, Y., Zhong, F., Alrawais, A., Gong, B., Cheng, X., 2020. FlowGuard: an intelligent edge defense mechanism against IoT DDoS attacks. IEEE Internet Things J. 7 (10), 9552–9562.

Kashyap, A., Jain, A.K., 2021. Analysis of machine learning and deep learning approaches for DDoS attack detection on internet of things network. In: Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences. Algorithms for Intelligent Systems.

Kentik, "Kentipedia DDoS detection," 30 July 2021. [Online]. Available: https://www.kentik.com/kentipedia/ddos-detection. [Accessed 2021].

Kolias, C., Kambourakis, G., Stavrou, A., Voas, J., 2017. DDoS in the IoT: mirai and other botnets. Cybertrust 50 (7), 80–84 July.

Kotey, S.D., Tchao, E.T., Gadze, J.D., 2019. On distributed denial of service current defense schemes. Technologies 7 (19), 1–24 30 January.

Kovacs, E., "Google targeted in record-breaking 2.5 Tbps DDoS attack in 2017," 19 October 2020. [Online]. Available: https://www.securityweek.com/google-targeted-record-breaking-25-tbps-ddos-attack-2017. [Accessed 2021].

Kumar, P., Bagga, H., Netam, B.S., Uduthalapally, V., 2021. SADIoT: security analysis of DDoS attacks in IoT networks. Wirel. Personal Commun. 1–22 25 August.

Lau, F., Rubin, S.H., Smith, M.H., Trajković, L., 2000. Distributed denial of service attacks. In: SMC 2000 conference proceedings. 2000 IEEE International Conference on Systems, Man and Cybernetics. 'Cybernetics Evolving to Systems, Humans, Organizations, and Their Complex Interactions' (cat. no.0), Nashville, TN, USA, pp. 2275–2280.

Li, L., Zhou, J., Xiao, N., 2007. DDoS attack detection algorithms based on entropy computing. In: Proceedings of the International Conference on Information and Communications Security: ICICS 2007, 4861, Berlin, Heidelberg, pp. 452–466.

Li, J., Liu, M., Xue, Z., Fan, X., He, X., 2020. RTVD: a real-time volumetric detection scheme for DDoS in the internet of things. IEEE Access 8, 36191–36201 17 February.

Li, J., Lyu, L., Liu, X., Zhang, X., Lyu, X., 2021. FLEAM: a federated learning empowered architecture to mitigate DDoS in industrial IoT. IEEE Trans. Ind. Inf. 1–14.

Lohachab, A., Karambir, B., 2018. Critical analysis of DDoS—an emerging security threat over IoT networks. J. Commun. Inf. Netw. 3 (3), 57–78 September.

Mahjabin, T., Xiao, Y., Sun, G., Jiang, W., 2017. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. Int. J. Distrib. Sens. Netw. 13 (12), 1–33.

Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I., 2015. Internet of things (IoT) security: current status, challenges and prospective measures. In: Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, pp. 336–341.

Manavi, M.T., 2018. Defense mechanisms against distributed denial of service attacks: a survey. Comput. Electr. Eng. 72 (2018), 26–38.

Maria, G., "How to prevent a DDoS attack—6 strategies for small businesses," November Month 2020. [Online]. Available: https://www.getapp.com/resources/how-to-prevent-a-ddos-attack/. [Accessed June 2021].

McDermott, C.D., Majdani, F., Petrovski, A.V., 2018. Botnet detection in the internet of things using deep learning approaches. In: Proceedings of the International Joint Conference on Neural Networks (IJCNN). Rio de Janeiro, Brazil.

Micro, T., "Into the battlefield: a security guide to IoT botnets," 19 Decenber 2019. [Online]. Available: https://www.trendmicro.com/vinfo/in/security/news/internet-of-things/into-the-battlefield-a-security-guide-to-iot-botnets. [Accessed 4 June 2021].

Misra, S., Krishna, P.V., Agarwal, H., Saxena, A., Obaidat, M.S., 2011. A learning automata based solution for preventing distributed denial of service in internet of things. In: Proceedings of the International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Dalian, China, pp. 114–122.

Molvizadah, V., "DNS Amplification DDoS Attack," 22 September 2016. [Online]. Available: https://medium.com/@vasiqmz/dns-amplification-ddos-attack-d4957b45bc66. [Accessed 17 March 2022].

Munshi, A., Alqarni, N.A., Almalki, N.A., 2020. DDoS attack on IoT devices. In: Proceedings of the 3rd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, pp. 1–5.

Nazario, J., 2008. DDoS attack evolution. Netw. Secur. 2008 (7), 7–10 July.

Noor, M.b.M., Hassan, W.H., 2019. Current research on Internet of Things (IoT) security: a survey. Comput. Netw. 148, 283–294 November.

Oyekunle, I., "What are the types of DDoS attacks?," 21 Septembet 2021. [Online]. Available: https://securitygladiators.com/threat/ddos/type/. [Accessed 17 March 2022].

Palepu, A., "WazirX server crashes as trading volumes surge,", 5 April 2021. [Online]. Available: https://www.medianama.com/2021/04/223-wazirx-server-trading-volume-token/. [Accessed 31 March 2022].

Pande, S.D., Khamparia, A., 2019. A review on detection of DDoS attack using machine learning and deep learning techniques. Think India J. 22 (16), 2035–2043 August.

Pateriya, R., Sharma, S., 2011. The evolution of RFID security and privacy: a research survey. In: Proceedings of the International Conference on Communication Systems and Network Technologies, Katra, India, pp. 115–119.

Prasad, K.M., Reddy, A.R.M., Rao, K.V., 2014. DoS and DDoS attacks: defense, detection and traceback mechanisms -a survey. Glob. J. Comput. Sci. Technol. Netw. Web Secur. 14 (7), 15–32.

Prasad, M.D., V, P.B., Amarnath, C., 2019. Machine learning DDoS detection using stochastic gradient boosting. Int. J. Comput. Sci. Eng. 7 (4), 157–166 April.

Pratt, M.K., "How an IoT botnet attacks with DDoS and infects devices," 09 June 2020. [Online]. Available: https://internetofthingsagenda.techtarget.com/feature/How-an-IoT-botnet-attacks-with-DDoS-and-infects-devices. [Accessed June 2021].

Ravi, N., Shalinie, S.M., 2020. Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. IEEE Internet Things J. 7 (4), 3559–3570 February.

Raza, A., 2021. Russian Internet Giant Suffers Largest DDoS Attack in History. Koddos 17 September[Online]. Available: https://blog.koddos.net/russian-internet-giant-suffers-largest-ddos-attack-in-history/.

Rieck, K., Holz, T., Willems, C., Düssel, P., Laskov, P., 2008. Learning and classification of malware behavior. In: Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, 5137, Berlin, Heidelberg, pp. 108–125.

RioRey, "Taxonomy of DDoS Attacks," 2015. [Online]. Available: https://www.riorey.com/types-of-ddos-attacks. [Accessed June 2021].

Robinson, S., "Mitigating risk: basic measures to prevent DDoS attacks in 2021," 9 April 2021. [Online]. Available: https://www.iot-now.com/2021/04/09/109089-mitigating-risk-basic-measures-to-prevent-ddos-attacks-in-2021/. [Accessed June 2021].

Roohi, A., Adeel, M., Shah, M.A., 2019. DDoS in IoT: a roadmap towards security & countermeasures. In: Proceedings of the 25th International Conference on Automation and Computing (ICAC), Lancaster, UK, pp. 1–6.

Rudman, L., Irwin, B., 2015. Characterization and analysis of NTP amplification based DDoS attacks. In: Proceedings of the Information Security for South Africa (ISSA), Johannesburg, South Africa, pp. 1–5.

Salim, M.M., Rathore, S., Park, J.H., 2020. Distributed denial of service attacks and its defenses in IoT: a survey. J. Supercomput. 2020 (76), 5320–5363.

Shafiq, M.Z., Ji, L., Liu, A.X., Pang, J., Wang, J., 2012. A first look at cellular machine–to-machine traffic: large scale measurement and characterization. ACM SIGMETRICS Performance Evaluation Review 40 (1), 65–76.

Shafiq, M., Tian, Z., Sun, Y., Du, X., Guizani, M., 2020. Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. Future Gener. Comput. Syst. 107, 433–442 June.

Shah, T., Venkatesan, S., 2019. A method to secure iot devices against botnet attacks. In: Proceedings of the International Conference on Internet of Things ICIOT, 11519, Cham, pp. 28–42.

Shapelez, A., "Mēris botnet, climbing to the record," 9 September 2021. [Online]. Available: https://habr.com/en/company/yandex/blog/577040/. [Accessed October 2021].

Sharafaldin, I., Lashkari, A.H., Hakak, S., Ghorbani, A.A., 2019. Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In: Proceedings of the International Carnahan Conference on Security Technology (ICCST), pp. 1–8.

Sharma, D.K., Dhankhar, T., Agrawal, G., Singh, S.K., Gupta, D., Nebhen, J., Razzak, I., 2021. Anomaly detection framework to prevent DDoS attack in fog empowered IoT networks. Ad Hoc Netw. 121, 1–9 July.

Shurman, M., Khrais, R., Yateem, A., 2020. DoS and DDoS attack detection using deep learning and IDS. Int. Arab J. Inf. Technol. 17 (4A), 655–661 June.

Sicari, S., Rizzardi, A., Miorandi, D., Coen-Porisini, A., 2018. REATO: rEActing TO denial of service attacks in the internet of things. Comput. Netw. 137, 37–48 June.

Silva, F.S.D., Silva, E., Neto, E.P., Lemos, M., Neto, A.J.V., Esposito, F., 2020. A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios. Sensors 20 (3078), 1–28 may.

Singh, R., Tanwar, S., Sharma, T.P., 2020. Utilization of blockchain for mitigating the distributed denial of service attacks. Secur. Priv. 3 (3), 1–13.

Sonar, K., Upadhyay, H., 2014. A survey: dDoS attack on internet of things. Int. J. Eng. Res. Dev. 10 (11), 58–63.

Srinivasan, K., Mubarakali, A., Alqahtani, A.S., Kumar, A.D., 2019. A survey on the impact of DDoS attacks in cloud computing: prevention, detection and mitigation techniques. In: Proceedings of the ICICV 2019: Intelligent Communication Technologies and Virtual Mobile Networks, 33, pp. 252–270.

Tao, Y., Yu, S., 2013. DDoS attack detection at local area networks using information theoretical metrics. In: Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, VIC, Australia, pp. 233–240.

Taylor, S., 2013. The next generation of the internet revolutionizing the way we work, live, play, and learn. CISCO Point View 12 (6).

Tiana, Z., Li, M., Qiu, M., Sun, Y., Su, S., 2019. Block-DEF: a secure digital evidence framework using blockchain. Inf. Sci. 491, 151–165 (Ny)July.

Toulas, B., "Linux malware sees 35% growth during 2021," 15 January 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/linux-malware-sees-35-percent-growth-during-2021/. [Accessed 30 March 2022].

Tushir, B., Dalal, Y., Dezfouli, B., Liu, Y., 2020. A quantitative study of DDoS and E-DDoS attacks on WiFi smart home devices. IEEE Internet Things J. 8 (8), 6282–6292 April.

Tv, I., "CBSE website crashes after Board declares Class 12 exams result 2020," 13 July 2020. [Online]. Available: https://www.indiatvnews.com/education/exam-results-cbse-class-12-result-declared-cbse-website-crashes-after-class-12-board-exam-results-announced-633822. [Accessed 01 April 2022].

Ubale, T., Jain, A.K., 2018a. SRL: an TCP SYNFLOOD DDoS mitigation approach in software-defined networks. In: Proceedings of the International Conference on Electronics, Communication and Aerospace Technology (ICECA). Coimbatore, India.

Ubale, T., Jain, A.K., 2018b. Taxonomy of DDoS Attacks in Software-Defined Networking Environment. Proceedigns of the FTNCT 2018: Futuristic Trends in Network and Communication Technologies, Communications in Computer and Information Science in.

Vailshery, L.S., "Global IoT end-user spending worldwide 2017–2025," 22 January 2021. [Online]. Available: https://www.statista.com/statistics/976313/global-iot-market-size/. [Accessed June 2021].

Vasques, A.T., Gondim, J.J., 2019. Amplified reflection DDoS attacks over IoT mirrors: a saturation analysis. In: Proceedings of the Workshop on Communication Networks and Power Systems (WCNPS), Brasilia, Brazil, pp. 1–6.

Vishwakarma, R., Jain, A.K., 2019. A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks. In: Proceedings of the 3rd International Conference on Trends in Electronics and Informatics (ICOEI). Tirunelveli, India.

Vishwakarma, R., Jain, A.K., 2020. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommun. Syst. 73 (1), 3–25.

Yu, X., Yu, W., Li, S., Yang, X., Chen, Y., Lu, H., 2021. WEB DDoS attack detection method based on semisupervised learning. Secur. Commun. Netw. 2021, 1–10.

Yuan, X., Li, C., Li, X., 2017. DeepDefense: identifying DDoS attack via deep learning. In: Proceedings of the International Conference on Smart Computing (SMARTCOMP), Hong Kong, China, pp. 1–8.

Zare, H., Azadi, M., Olsen, P., 2017. Techniques for detecting and preventing denial of service attacks (a systematic review approach). Information Technology - New Generations, Advances in Intelligent Systems and Computing 558, 151–157. https://doi.org/10.1007/978-3-319-54978-1_21.

Zargar, S.T., Joshi, J., Tipper, D., 2013. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Commun. Surv. Tutor. 15 (4), 2046–2069.

Zhang, C., Green, R., 2015. Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network. Soc. Model. Simul. Int. 8–15.

Zhang, W., Qu, B., 2013. Security architecture of the Internet of Things oriented to perceptual layer. Int. J. Comput. Consum. Control (IJ3C) 2 (2), 37–45.

Pooja Kumari is a Ph.D. scholar in National Institute of Technology, Kurukshetra, India. She has received her M.Tech degree in Computer Science and Technology (Cyber Security) from Central University of Punjab, Bathinda, India. Her research interests include, IoT Security, Machine Learning and Deep Learning, Network and Information Security.

Dr. Ankit kumar Jain is presently working as Assistant Professor in National Institute of Technology, Kurukshetra, since September 2013. He received Master of technology from Indian Institute of Information Technology Allahabad (IIIT) India . Dr. Jain received PhD degree from National Institute of Technology, Kurukshetra in the area of Information and Cyber Security. He has more than 50 research papers in International journals and conferences of high repute including Elsevier, Springer, Taylor & Francis, Inderscience, IEEE, etc. His-general research interest is in the area of Information and Cyber security, Phishing Website Detection, Web security, Mobile Security, IoT Security, Online Social Networks and Machine Learning.