A Review of DDoS Attacks and Defenses in IoT

Wasif Islam[1], Suriani Mohd Sam[2]*, Hafiza Abas[3], Noraimi Shafie[4], Norliza Mohamed[5], Al Nuaimi Mohammed Fahad Ali[6]

[1,2,3,4,5,6]Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia,54100 Kuala Lumpur
[1]mdislam@graduate.utm.my,[2]suriani.kl@utm.my, [3]hafiza.kl@utm.my,[4]noraimi.kl@utm.my, [5]norlizam.kl@utm.my,[6]mohammed.al@graduate.utm.my

Article history

Received:
13 Sept 2022

Received in revised form:
29 Nov 2022

Accepted:
1 Dec 2022

Published online:
15 Dec 2022

*Corresponding author
suriani.kl@utm.my

Abstract

The velocity at which the Internet of Things is becoming the norm is disturbing. People now could independently interact with our surroundings on a wide range of platforms from almost anywhere on the earth. Due to its nature, IoT security is only average. Other reasons like obsolete software, insufficient encryption, a lack of resources, and others all play a role in this. When you add this to how commonplace it is, it is an easy target for online thieves. An intentional attempt to stop a targeted server, service, or network's normal flow by saturating the target or its surrounding infrastructure with Internet traffic is known as a distributed denial-of-service (DDoS) assault. Defense against DDoS on the Internet of Things has become a pressing area of research as a result of recent incidents, including the alleged crash of several well-known servers in the years prior. This paper examines the numerous DDoS assault techniques used by attackers and offers security countermeasures. It also discusses obstacles and issues that must be resolved for a more effective response.

Keywords: *IoT, DDoS, Botnet, Malware*

1. Introduction

The Internet of Things, or IoT, is a network of interconnected computing devices, mechanical and digital machinery, items, animals, or people that have unique identities (UIDs) and the capacity to send data over a network without the need for human-to-human or human-to-computer contact [1]. According to Statista, the globe has over 21.5 billion networked gadgets. Their number is expected to skyrocket in the coming years as internet usage grows and new devices and technology enter the market. IoT, on the other hand, will be essential to civic and industrial infrastructure. It encompasses devices in many aspects of life [2]. Although IoT is simple in nature, it becomes considerably more intricate and significant when dealing with security and privacy concerns. By having untrustworthy networking protocols and less human interaction it becomes more exposed to different security vulnerabilities. IoT devices are usually constrained in terms of both power resources and memory and thus lack the essential built-in security to combat such threats. Aside from the technological elements, people also contribute to the susceptibility of the devices to modern day attacks. As IoT becomes smarter by the day, security must get smarter as well to deal with newer

* *Corresponding author. suriani.kl@utm.my*

and smarter varieties of threats. A denial-of-service (DoS) attack overloads a server, rendering a website or resource inaccessible. A distributed denial-of- service (DDoS) attack is a type of DoS attack that employs numerous computers or machines to overwhelm a specific resource.

Both types of attacks aim to overwhelm a server or online application in order to disrupt services. It is a real-world scenario where an unforeseen traffic bottleneck has jammed the roadway, preventing ordinary traffic from reaching its destination. An attacker exploits vulnerability of IoT devices by making them a “bot” using malicious software or malware that allows the attacker to command the devices. These bots are then coordinated in a network, thus giving birth to the term “botnet” and then coordinate them to perform a DDoS attack on the target to interrupt its regular service. DDoS in IoT generally takes place in application layer and infrastructure layer of the network architecture.

2. Denial-of-Service(DoS)

A denial-of-service (DoS) attack overloads a server, rendering a website or resource inaccessible. A distributed denial-of-service (DDoS) attack is a type of DoS attack that employs numerous computers or machines to overwhelm a specific resource. Both types of attacks aim to overwhelm a server or online application to disrupt services. It is a real-world scenario where an unforeseen traffic bottleneck has jammed the roadway, preventing ordinary traffic from reaching its destination. An attacker exploits vulnerability of IoT devices by making them a “bot” using malicious software or malware that allows the attacker to command the devices. These bots are then coordinated in a network, thus giving birth to the term “botnet” and then coordinate them to perform a DDoS attack on the target to interrupt its regular service. Here is how DDoS attacks are gaining notoriety as of late.

1. The coronavirus pandemic forced everyone online in Q3 of 2021 and has beaten all records in terms of daily attacks [3].
2. Statistics show that there is over a 100% increase in attacks compared to the previous year with modern attack vectors targeting different network layers. [4]
3. Targets of DDoS attacks ranges from healthcare, businesses, gaming applications and so on. 4.As technology advances, there is prospect of DDoS attacks reaching new heights.
4. DDoS attacks are now sold at the dark web for as little as $10 per hour up to $60 per hour and goes higher with more “power” [5].
5. A recent study by Kaspersky Lab revealed that a DDoS attack can cost a company over $1.6 million. [6]
6. By having services down, consumers tend to lose trust and confidence in the business.
7. DDoS can be used as a distraction or “smokescreen” to divert attention of the security staff while other malicious attacks are taking place i.e., Data Theft.’

3. Threat in DDoS

A common theme in the studies of DDoS when it comes to IoT is security. There are reviews and surveys detailing about the threats and solutions DDoS possess in

IoT. However, they are scarce and have been around for a while. IoT technologies are evolving fast, there are rapid developments and implementation in all layers of IoT which introduces newer security issues requires newer studies on the matter. Vishwakarma et al. [7] wrote a survey which covers Security issues, taxonomy of DDoS attacks, role of IoT with botnets and malware, the defense mechanisms and provides challenges and issues. Authors of [8] presented a much more recent impact evaluation of DDoS attacks on IoT devices, which sheds new light to this field. Most of the recent studies focus on the defense mechanisms and DDoS detection is a common theme. Ali et al. [8] shows that the contribution of studies in botnet detection in IoT is almost twice as the contribution in its avoidance. It is worth noting that, while these studies help to improved security, they also provide vital knowledge to cyber criminals who are able to learn and adapt to protections and devise workarounds. The Internet of Things has made it much easier for bad actors to devise new techniques. As it improves at a rapid pace and technology evolves, some protection systems must be reviewed to verify their efficacy. With the introduction of fresh approaches, it is critical to examine them and design stronger defenses. This review will contribute by analysing different approaches and issues that need to be resolved in order to offer a suitable defense against DDoS attacks in an IoT setting.

4. BOTNETS In IoT

The earliest botnets were desktop computer that were a bunch of personal computers infected with software that would be controlled as a group by a malicious actor. With the advent of IoT, it has become a contributing factor to perform large scale DDoS attacks. IoT botnets are well-known for performing distributed denial-of-service (DDoS) attacks against target companies to impair their operations and services. The critical role that routers play in networks creates new potential for bad actors to employ IoT botnets to launch more devastating cyberattacks. IoT botnets are sold on underground forums, indicating how easy they can be obtained by cybercriminals. Modern botnets are self- replicating in nature. Malwares are designed such that the botnets can multiply in the network or devices within its reach.

IoT systems consists of several devices that are linked to one another, making it easy to infect new devices and expand the number of botnets. IoT visions a world where everything is connected and for that to happen devices are required to be always interconnected, much like the internet itself. Botnets are often administered by a single command-and-control (C&C) server that is linked to all infected devices. However, the use of peer-to-peer (P2P) networking in some botnets eliminates the requirement for a command and control (C&C) server, making it more difficult to shut them down. Most of the IoT botnets that exist today are based on IoT malware codebases as shown in Figure 1.

The similarities between these codebases reveal the underlying nature of IoT botnets and how they work.

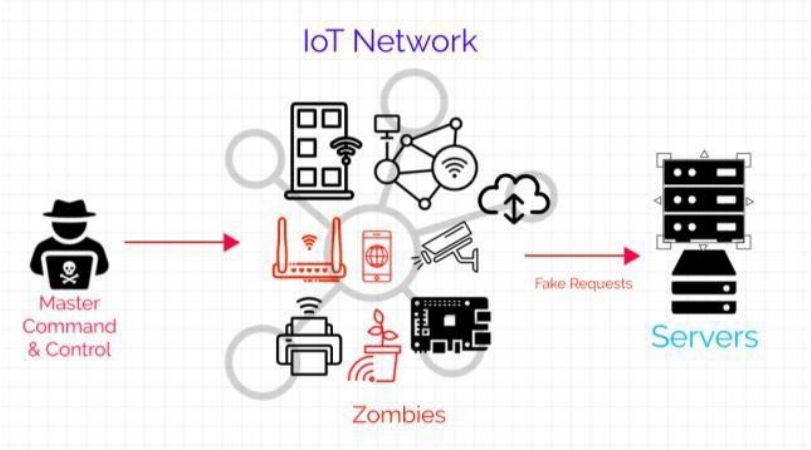

Figure 1. IoT network being used as a weapon to perform DDoS [2]

4.1 Kaiten

Also known as Tsunami, has been around two decades now [9] is popular among cybercriminals and amateur hackers mostly due to being open source and easily accessible. The malware spreads by brute forcing Telnet services and tries connecting to random public addresses with a preset of login credentials [10]. Interestingly, the modern variants of Kaiten have a bot-removing feature that removes any other present infections so it can be the only one in command.

4.2 Mirai

The most notable malware responsible for the event in 2016 caused so much damage that it took the world by a storm using IoT-powered DDoS attack. It was developed as a for-sale DDoS tool and was used to target gamers. After the 2016 incident, current forms of the Mirai botnets could clean up infections and completely monopolize a device.

4.3 Mozi

Just like the previous two mentioned malware, Mozi also relies on weak passwords on Telnet services. Mozi targets routers and IoT devices alike. It tampers with the web traffic that redirects users to malicious sites. Addition to that, it uses clever techniques that are specifically adapted to various architectures. This helps Mozi operators to prevent having their malware deleted on a device reboot and to lengthen dwell periods on infected devices [13], it is a defense mechanism to prevent being “cleaned” from other like-natured malwares as mentioned in the previous section.

4.4 Worm War

The malware instances above depict a pattern of "war" amongst botnet malwares over vulnerable devices, all while competing silently and unnoticed to the device owners [12]. Many of the threats posed by IoT botnets today persist because users fail to detect infected devices or are unable to clean the devices themselves. IoT botnet malware families and variations have the capability of infecting as many

devices as possible while cancelling out other botnet infections. The current worm battle demonstrates how ambitious IoT botnet operators are in building the ultimate botnet army, and how users can be caught in the crossfire inadvertently.

5. DDoS In IoT

The DDoS attack landscape shifts and evolves from season to season, the underlying reality remains constant: as a relatively simple and widely available tactic, DDoS attacks will always be popular among hackers. In order to defend against DDoS assaults, it is essential to understand how they operate at different IoT layer depths. There are endless attacks, and the list would never end, but the next section will highlight the most notorious ones. Figure 2 shows the distribution of DDoS attacks by duration of Q2 and Q3 in 2021. This list consists of most of the notorious attacks and how they work as elaborated below.

5.1 Application Layer Attack

Application layer DDoS in IoT are attacks intended to target the application itself, concentrating on specific vulnerabilities or faults that prevent the application from delivering content to the user. Application layer DDoS attacks are intended to target specific applications, the most popular of which are web servers. The most problematic aspect of application layer DDoS attacks is that, even when multi-vector attacks contain detectable patterns, a determined attacker will monitor the outcomes of his attack and adapt it to thwart a trained and determined defense. Because active attackers are known to constantly vary payload patterns to circumvent simple DDoS mitigation, keeping an ongoing list of known attack patterns soon becomes impracticable owing to scalability difficulties and the rate at which this list must be updated. Furthermore, because payload patterns pose a high danger of inflicting collateral harm, keeping a long-lived set of payload patterns may be counterproductive. Examples of application layer includes:

(1) Targeting DNS Server - DNS queries are sent via IoT botnets. If the attacker intended to target a DNS server, he would use all his botnet “zombies” to send DNS request messages for an amplification record from open recursive DNS servers, which convert domain names into IP addresses. When a new request arrives, the server immediately sends its own request to an infected server to retrieve the amplification record. This attack is carried out by spoofing, such that the server in inundated with answers even though no requests were ever submitted.

(2) HTTP Flood Attack - This type of DDoS attack made to overload specific parts of a site or server. They are complex and hard to detect because the sent requests look like legitimate traffic. These requests consume the server’s resources causing the site to go down. These requests can also be sent by bots, increasing the attack’s power.

5.2 Infrastructure Layer Attack

As the name suggests, it targets the infrastructure layer to stop systems from performing normally by exploiting vulnerabilities. They come in two forms.

Resources based - To carry out such an attack, hackers use a large number of computers and internet connections (IoT) to flood a website with traffic, clogging up the website's available bandwidth. As a result, genuine traffic is blocked, and hackers can effectively take down the website. Bits per second are used to measure volume-based attacks (bps).

1. ICMP floods - Attackers bombard the server with faked ICMP packets from many source IP addresses (think IoT). As a result of this attack, server resources are depleted and requests are unable to be processed, forcing the server to shut down or having a significant impact on its

performance. ICMP flood attacks can be directed at specific servers, or they can be distributed at random. It effectively drains bandwidth till it is depleted.

2. Ping floods - Attackers flood the server with fake ping packets from many source IP addresses. It is a development of ICMP flood attacks. The attacker's goal is to overwhelm the server until it goes down. The most serious disadvantage of this attack for website owners is that it can be difficult to detect, often masquerading as legitimate traffic.

Protocol based - Protocol attacks, as opposed to volume- based attacks, seek to deplete server resources rather than bandwidth. They also target "intermediate communication devices," which are mediators between the server and the website, such as firewalls and load balancers. To use the available resources, hackers overwhelm websites and server resources by sending bogus protocol requests. The effectiveness of these attacks is assessed in packets per second (pps) as shown in Figure 2.

1. Ping of Death - Attackers manipulate IP protocols by sending malicious pings to a server. The server will reboot or completely crash because of this attack. That is precisely why a DoS attacks should not be underestimated: a single attacker might bring a data center to a halt.
2. SYN Flood - Attackers make use of vulnerabilities in the three-way handshake of a Transmission Control Protocol (TCP) connection, which is the communication process between the client, the host, and the server. Attackers transmit faked SYN packets to the targeted server until the server's table memory connection is depleted, forcing the entire service to shut down.

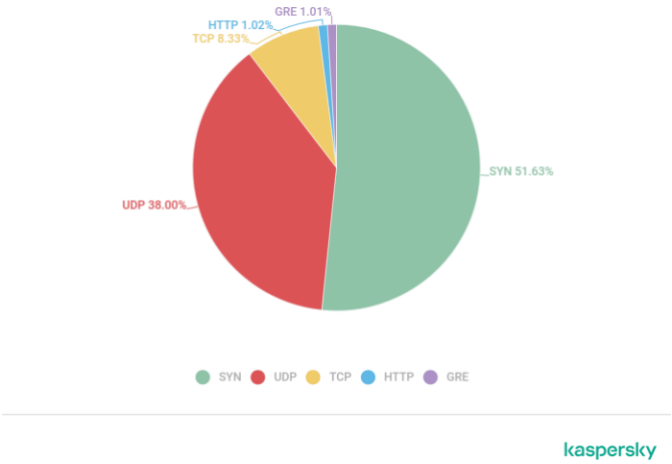

Figure 2. Distribution of DDoS attack types in quartiles of 2021 from Kaspersky [6].

5.3 Network Layer Attack

The attacker targets the IoT device by taking advantage of the vulnerabilities discovered at this layer. The RPL protocol is intended for IoT devices to minimize energy usage by traffic flow techniques such as point-to-point, point-to-multipoint, and multipoint to point.

1. Wormhole Attack - The aim behind this attack is to use a tunnel to send data from one compromised node to another malicious node at the other end of the network. This attack can be coordinated with the Sybil attack to be more effective.
2. Sybil Attack – A Sybil attack is a sort of computer network service attack in which an attacker subverts the reputation system of the service by generating a large number of pseudonymous identities and using them to obtain disproportionately great influence. Combining these two attacks pose a severe threat especially to IoT systems.

6. Defense against DDoS in IoT

The procedure of guarding against DDoS is classified into four stages. The first is detection, which employs a variety of approaches to discover anomalies on the network. As attacks get more sophisticated, detection must incorporate novel methodologies [14] that can identify an incoming DDoS attack in real time. Following identification, the logical next step is preventive to ensure that the damage is restricted or avoided entirely if feasible. Mitigation aids in reducing the impact of DDoS attacks [15]. Finally, analysis is essential for retrieving information from logs to increase resilience. The next part will go over and explain some of the most essential defense mechanisms and tactics.

a) Botnet Detection with Machine Learning on IoT devices

Machine learning is superb when it comes to classification of data. Therefore, it is a go-to approach when it comes to detection techniques for malware strains. The authors of [16] provide a machine learning-based detection system that analyses packet flow with high attack detection accuracy.

However, most IoT-devices are low-powered, but this study
[17] presents a machine learning technique that is computationally less intensive, making it ideal for IoT device implementation. The authors of [22] proposes a system where the network is monitored to detect any anomalies in IoT using deep learning algorithms namely convolutional neural network model is validated using the “Bot-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, and IoT-23" intrusion detection datasets.

b) Honeypot DDoS Defense

As Figure 3 illustrates honeypots are a form of deception technique that helps to figure out how attackers behave. Honeypots can be used by security teams to investigate cybersecurity breaches and get information on how fraudsters work. When compared to typical cybersecurity measures, they also lower the likelihood of false positives because genuine activity is unlikely to be attracted. IoT can be used as honeypots which can be used to learn more about DDoS attacks [18]. Honeypots can also be used to mitigate DDoS attacks by redirecting most of the assault to the false systems while repairs and fixes are being implemented. This research explores in depth on how the mitigation works by routing attacks from servers at ISP level [19].

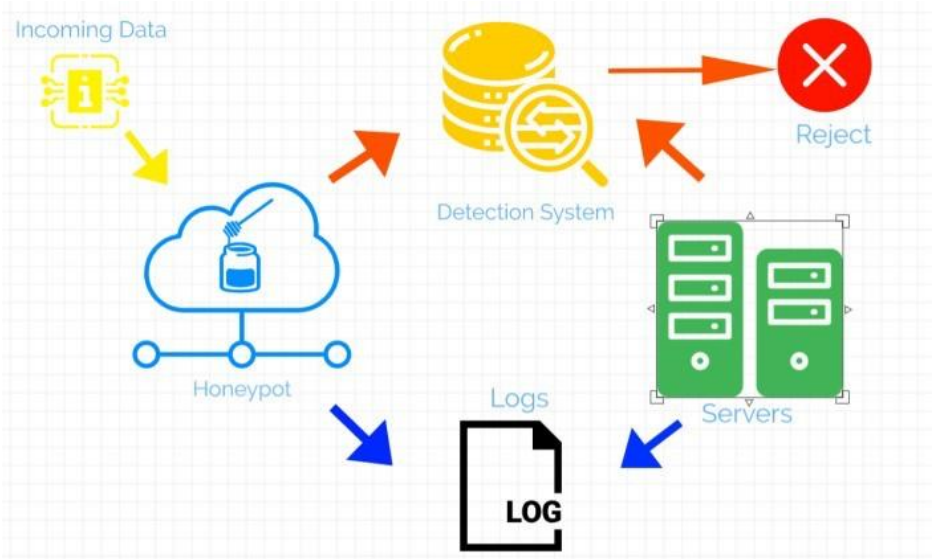

Figure 3. Distribution of DDoS attack types in quartiles of 2021 from Kaspersky [6].

c) Blockchain DDoS Defense

When it comes to storing data on the network, blockchains are transparent and decentralized. There is no single point of failure as a result of this. As mentioned in the preceding section, it may be a solution to resource exhaustion-based DDoS attacks [20]. DDoS attacks are thwarted by blockchain's immutability, integrity, anonymity, and verifiability and much more.

Table 1: Summary for DDoS defense mechanisms

Solution	Advantages	Drawbacks	Use Case
Honeypots	Best known for trapping newer models of malwares especially in IoT. [3]	Advanced malwares have built- in features that lets it known about Honeypots. Highly cost intensive to counter the above.	IoT Honeypot based DDoS defense systems. [18]
Machine Learning	Newer algorithms are quite effective [17] to detect anomalies in the network with desired precision	Becomes more computationally heavy and burns up more resources with higher accuracy.	Anomaly detection using deep learning.
Blockchain	Being decentralized it becomes hard for DDoS to target a single point, making the defense distributed also.	It is completely reliant on miners to maintain security at all times, making it a specialized solution to a difficult-to-implement problem	Smart Contract platform by Ethereum Gas system

7. Discussions

DDoS attacks are destructive to systems that aren't prepared. This is a reality that cyber criminals are aware of, and they make good use of it. Therefore, defense should be ready for everything and have numerous aces up their sleeves in case the worst happens, since this will reduce damage. The defense systems should be divided into multiple steps namely, detection, prevention, mitigation, and analysis. Development of such defense needs to be prioritized according to the popularity of the attack. "IoT's biggest benefit is also its worst disadvantage." Even with all the research and studies in this field there seems to be an upward trend in DDoS attacks. Despite the solutions covered in the previous sections there are still countermeasures that can be employed:

1. Raise Firewalls: They are the first line of security, yet they are frequently disregarded. It's a simple way to ensure a network's security. A properly implemented firewall can prevent malwares from forming a botnet.
2. Patch Firmware: Because IoT devices exist in so many different shapes and sizes, most manufacturers don't bother to send out current security upgrades and fixes. This gives attackers to an advantage of new or old vulnerabilities and create new DDoS versions. The point is to make it harder for bad actors, the harder it is for them, the better it is for us.
3. Change Passwords: Default passwords are commonly used on IoT devices. Changing to a stronger password is convenient for manufacturers and a minor inconvenience for consumers. Human errors are always a target for attackers. The aftermath of changing the default password on the recently purchased Raspberry Pi 3 can lead to contributing to the botnets.

4. Setting Limits: Home network management, Internet Service Providers, Government can implement detection mechanisms at their ends to ensure the attack is prematurely thwarted before the damage is done to the target.

8. Conclusions

This review presents motivations for attackers to use IoT devices to launch DDoS attacks. From classic approaches to IoT-specific ones, it examines the ideas involved in protecting against a DDoS attack. During the journey of writing this review, I have come across multiple research and studies that are coming up and clever implementation of security systems to deal with such attacks. Even so,the DDoS attacks in the field of IoT are still on the rise. The development of new technologies is pavingthe way for attackers to come up with clever attack vectors, in response, researchers will adapt andemploy better systems. The situation represents the game of cat and mouse. This paper haspresented the various attacks and how attackers combine multiple attack vectors to target systems.It also reviews various defense mechanism that have been researched and studied, by listing their effectiveness and drawbacks in a real-world scenario. As devices get smarter, so does the attacks, it goes without mentioning that we need to implement smarter solutions to combat them.

References

[1] Alexander S. Gillis, “What is internet of things (IoT)?” Tech Target, August 2021.
[2] Nick G., “How Many IoT Devices Are There in 2021?” November 1, 2021.
[3] Alexander Gutnikov, Oleg Kupreev, Yaroslav Shmelev, “DDoS attacks in Q3 2021 - DDOS Reports”, 08 Nov 2021
[4] David Warburton, “DDoS Attack Trends for 2020”, F5Labs, Threat Intelligence, May 07, 2021.
[5] The Dark Web: DDoS Attacks Sell for as Low as $10 Per Hour, Mission Critical, August 26, 2020.
[6] Distributed Denial of Service: Anatomy and Impact of DDoS Attacks, Kaspersky USA 2021.
[7] Ankit Kumar Jain, Ruchi Vishwakarma, “A survey of DDoS attacking techniques and defence mechanisms in the IoTnetwork, Springer Link, July 2019.
[8] Ali et al., "Systematic Literature Review on IoT-Based Botnet Attack," in IEEE Access, vol. 8, pp. 212220-21223
[9] Stephen Hilt, Fernando Mercês, Mayra Rosario, David Sanchokaiten.c, “Worm War: The Botnet Battle for IoTTerritory”, Trend Micro Research, Dec 27, 2001
[10] Shah Sheikh, “Kaiten Malware Returns to Threaten IoT”, Tara Seals Infosec Magazine Home, March 2016.
[11] Catalin Cimpanu, “New HEH botnet can wipe routers and IoT devices”, Zero Day, October, 2020
[12] CVE-2015-1328 Detail, National Vulnerability Database (NIST:NVD), September 2017.
[13] Khadijeh Wehbi; Liang Hong; Tulha Al-salah; Adeel A Bhutta, “A Survey on Machine Learning Based Detection onDDoS Attacks for IoT Systems, IEEE 2019 SoutheastCon, USA, April 2019.
[14] Kishan Patel, “A Survey: Mitigation of DDoS attack on IoT Environment”, 2019 IEEE International Conference onRobotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON), January 2018.
[15] Christopher D. McDermott, Farzan Majdani, Andrei V. Petrovski, “Botnet Detection in the Internet of Things usingDeep Learning Approaches”, 2018 International joint conference on neural networks (IJCNN 2018), July 2018.
[16] Doshi R, Apthorpe N, Feamster N, “Machine learning DDoS detection for consumer internet of things devices.
Cryptography and Security”, 2018 IEEE Security and Privacy Workshops (SPW), July 2018

[17] M. F. Razali, M. N. Razali, F. Z. Mansor, G. Muruti and N. Jamil, "IoT Honeypot: A Review from Researcher's Perspective," 2018 IEEE Conference on Application, Information and Network Security (AINS), 2018, pp. 93-98, doi:10.1109/AINS.2018.8631494.

[18] A. Sardana and R. C. Joshi, "Honeypot Based Routing to Mitigate DDoS Attacks on Servers at ISP Level," 2008 International Symposiums on Information Processing, 2008, pp. 505-509, doi: 10.1109/ISIP.2008.115.

[19] Wani, S.; Imthiyas, M.; Almohamedh, H.; Alhamed, K.M; Almotairi, S.; Gulzar, Y., "Distributed Denial of Service (DDoS) Mitigation Using Blockchain—A Comprehensive Insight", Symmetry 2021, 13(2), 227, doi.org/10.3390/sym13020227

[20] Sicari, S., Rizzardi, A., Miorandi, D., & Coen-Porisini, A., "REATO: REActing TO Denial-of-Service attacks in the Internet of Things. Computer Networks", Elsevier Computer Networks, Vol. 137, pp:37-48, June 2018.

[21] I. Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection inIoT Networks," in IEEE Access, vol. 9, pp. 103906-103926.