IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A MECHANISM FOR PREVENTING DDoS ATTACK OVER THE IoT NETWORKS

Miss. ANSARI ZUNAIRA BANO MOHAMMAD ANWAR

(INFORMATION TECHNOLOGY/COMPUTER SCIENCE)

(B. K. Birla College of Arts, Science & Commerce, Kalyan)

ABSTRACT

Nowadays, The Internet of Things (IoT) has made our lives more reliable and efficient in multiple ways. IoT is a rapidly emerging technology in the consumer, business, industrial, and social ecosystems. IoT networks use the communication technologies, such as IoT devices, to share and spread information applications and hardware. As such, Distributed Denial of Service attacks use multiple connected devices executed by botnets and creates many harmful and dangerous threats to the security of IoT networks. Attackers can analyze and attack IoT devices as part of botnets to launch DDoS attacks by taking advantage of their flaws and targeting the server by sending a flood of messages and creating internet traffic then the system halts and reduces the performance of the system. In this research, when an attacker sends a flood of fraud messages, then some alert notifications, warning messages, and alarms are triggered in the victim's machine to avoid data loss. Also includes secondary data (research papers, case studies, and past cybercrime studies) to detect the threats and prevent them in the network. This presenting paper throws light on the prevention and techniques of DDoS attacks in IoT.

Keywords: Internet of Things (IoT), Alert notification, Internet traffic, Distributed Denial of Service (DDoS) attack, Botnet.

• INTRODUCTION

IoT networks allow different devices to communicate and process information effectively. Despite their benefits, these networks are becoming more susceptible to DDoS attacks, which flood systems with fraudulent traffic, causing outages and monetary losses. Wireless networks are made available by IoT providers to link low-power devices that emit continuous data. The various techniques for preventing and identifying DDoS assaults in an Internet of Things setting are thoroughly examined in this research study. As the variety of Internet of Things (IoT) devices grows rapidly, network threats are becoming a bigger issue. According to recent reports, the most common and dangerous attacks in IoT networks are Distributed Denial of Service (DDoS) attacks.

These days, distributed denial of service (DDoS) assaults are one of the most potent yet little-known cybersecurity risks. It is a significant obstacle in IoT networks, which are regarded as one of the world's expanding issues. DDoS assaults follow various patterns. As a crucial component of IoT network defense systems, this threat underscores the importance of implementing network anomaly mitigation techniques, which further safeguard the devices because of their beneficial effects on our day-to-day activities. A DDoS occurs when a threat actor uses resources from multiple, remote locations, to attack an organization’s online operations, server, services, or network and devices and servers, often targeting the networking devices that establish a connection to the internet and infect multiple PCs. A DDoS attack can seriously damage a brand’s reputation and value and cost millions of dollars in revenue. Attackers and DDoS attacks are sometimes used for the misused purpose of distracting cybersecurity operations while other criminal activity, such as data theft or network infiltration. And in fraud cases to decrease the value of the business. So, we must stop it and find a solution so that most people can be saved from DDoS attacks.

A group of linked computers and gadgets that can interact with one another without human intervention is known as an Internet of Things network. There are Various types of computer networks can be distinguished by their operational size. Among them are:

- **LAN**: A network that covers a limited geographic region is known as a local area network (LAN). It's a network of several computers. It is utilized, for instance, in workplaces, buildings, institutions, etc.
- **MAN**: A network that covers a larger geographic region is known as a metropolitan area network (MAN). It is a grouping of many LANs. For instance, it is utilized in several cities.
- **WAN:** A wide area network (WAN) can be dispersed globally and is not restricted by geography. It consists of several LANs and MANs. For instance, it is utilized in several nations and states.
- **SAN:** A storage area network (SAN) is a fast network that links servers to storage devices.
- **CAN:** Without a host computer, a Controller Area Network (CAN) enables microcontrollers and other devices to interact with one another in applications.

- **PAN:** Data transfer between devices, including laptops, tablets, and personal digital assistants, that are situated in close proximity to a single user is accomplished through a personal area network, or PAN.
- **GAN:** A global area network (GAN) facilitates mobile connectivity over an indefinite number of satellite coverage regions, wireless LANs, etc.

Distributed Denial of Service (DDoS) attacks: DDOS attacks are malicious attempts to overload a targeted server, service, or network with overwhelming internet traffic in order to interfere with its regular operations. Large botnets are used by attackers to repeatedly transmit signals to your server. They cut off external traffic from your system. DDoS assaults come in three varieties:

1) Volumetric attack: Volume-based attacks aim to overload the capacity of the target network with large amounts of traffic [1].

2) Application layer attack: The target is attacked by the user in order to redirect HTTP, DNS, HTTPS, and SMTP web traffic. Troubleshooting this kind of assault is often detrimental [1].

3) Protocol attacks: It is also known as state-exhaustive attack. This attack targets the network layer and transport layer protocols using flaws in the protocol to overwhelm target resources [1].

• REVIEW OF LITERATURE

1. A comprehensive review of the literature has been conducted, identifying various techniques for the detection and prevention of DDoS attacks [2].
2. Additionally, we provide examples of DDoS attacks and their types, along with various detection and prevention strategies commonly used in IoT networks.
3. While some methods focus solely on detecting DDoS attacks, others are designed to prevent the attack sources from targeting IoT networks altogether.

• OBJECTIVES

1. To study the different types of IoT networks, devices, and technologies. Which makes the IoT environment more beneficial. Through which human beings get relief from their work.
2. To study DDoS attack and their types and to find out how DDoS attack is implemented to dominate IoT networks.
3. To analyze possible measures to prevent the DDoS attack from coming to the victim's machine and filling the loopholes to secure the information and data.
4. Understanding the multiple ways attackers might compromise your system is first the step toward preventing attacks.

• RESEARCH METHODOLOGY

This research paper has been written based on primary as well as secondary data. Both primary and secondary data have their significance based on the perpetration or purpose you can use them. This study integrates:

1. **Secondary Data**: Analyzing existing research papers, case studies, and cybercrime reports to identify DDoS types, vulnerabilities, and prevention techniques.
2. **Primary Data**: A survey of 73 respondents was conducted to assess awareness of IoT security and DDoS attack prevention. The dataset includes attributes such as age, IoT device usage, security awareness, and preventive measures.

Findings from Primary Data:

The survey analysis reveals:

1. **Knowledge of IoT Networks:** 85% of participants were familiar with IoT networks, indicating an understanding of connected devices and their applications in smart homes, healthcare, and industrial automation.
2. Preferred IoT Network Type: Wi-Fi (58%), GPS (14%), 4G (12%), 5G (10%), and Bluetooth (6%), each with distinct security challenges.
3. IoT Network Vulnerabilities: 72% acknowledged that IoT networks are highly susceptible to malware, cyber-attacks, and system corruption.
4. Incidents of Account Hacking: 53% reported experiencing account hacking incidents, reinforcing the need for enhanced authentication and security protocols.
5. System Performance Issues: 61% of users reported system slowdowns and halts, potentially due to malware infections or DDoS attacks.
6. Awareness of Cyber Threats: 80% agreed that attackers could steal sensitive data, emphasizing the need for encryption, anomaly detection, and network segmentation.
7. DDoS Attack Prevention Strategies: 74% recommended best practices such as reading notifications carefully, avoiding sharing OTPs/passwords, updating systems regularly, and installing firewalls.

Visualization:

1. A bar chart depicting IoT device usage distribution.
2. A pie chart representing DDoS awareness levels.

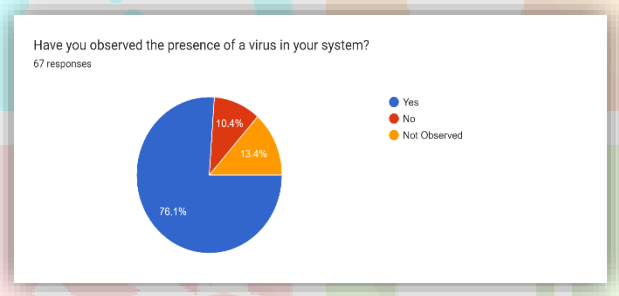
• SCOPE OF THE STUDY

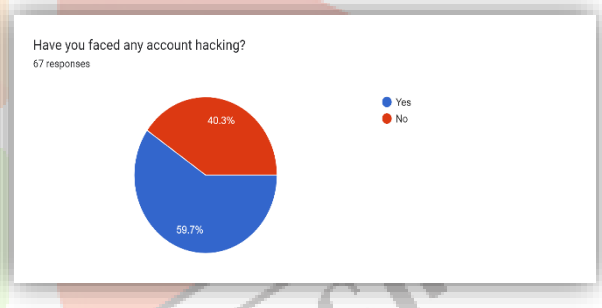
This paper gives clear ideas to help DDoS attacks and explains the different types of attacks & threats on IoT networks. It provides an overview of different types of computer networks. It also, explains how to identify DDoS attacks in IoT networks and save people from these attacks.

• DISCUSSION

` Numerous effects in our digital world are connected with networks, with one arising technology being the Internet of Things. Which connects two or more devices via the internet. IoT enables the development of computer different devices, smart devices, security, and the industrial or artificial sector. IoT devices communicate using IoT protocols. The Internet of Things network is also plagued with many different types of attacks, in which one of the most common and dangerous attacks is the DDoS attack.

The total number of DDoS assaults is encyclopaedically and is expected to double to 14.5 million by 2022[3]. A DDoS attack can cost up to 12000 dollars for a small company or more than 2 million dollars for a larger one with financial loss and a company reputation. Amazon web services, Quora, GitHub, Google, and online gaming services are affected by DDoS attacks. People now prefer to purchase online, but many are unaware that online risks are always evolving at an accelerated rate. Hackers are targeting new targets, developing new botnets, and executing more distributed denial of service assaults than ever before. Despite these risks, awareness among IoT users remains low, leaving many susceptible to virus attacks, account hacking, and other malicious activities. I conducted a survey on IoT networks and their DDoS attacks with 73 respondents to help people know about IoT networks and their malicious attacks. I analyze many people are victims of virus attacks and account hacking because of not know of these kinds of criminal activities or attacks. And also analyzes how users can detect or identify DDoS attacks on their systems and what advanced prevention techniques can be used to save from this.





SURVEY INSIGHTS AND ANALYSIS: To understand the extent of IoT security challenges, a survey was conducted among 73 respondents to assess their awareness of DDoS attacks and security measures. The key findings include:

- **Knowledge Gap**: A significant number of respondents demonstrated limited awareness of IoT-related threats, highlighting the need for educational initiatives.
- **IoT and Business Opportunities**: Many respondents acknowledged that IoT networks improve automation and reduce manual effort, but security risks such as DDoS attacks hinder these benefits.
- **Minimal Use of Security Tools**: Many users reported inadequate security measures, emphasizing the necessity of accessible, user-friendly, and cost-effective security solutions.
- **Communication Improvements via IoT**: While IoT enhances communication, concerns over data privacy and cyber threats persist, requiring robust security solutions.
- **Responses to Social Engineering Threats**: Some users still engage with fake calls or messages, highlighting the need for awareness programs to prevent phishing attacks.
- **Alignment with Secondary Data**: The survey results corroborate existing research that IoT devices remain highly vulnerable due to insufficient security measures.

Recommendations

The survey also explored methods for detecting and mitigating DDoS attacks on IoT systems. Based on the analysis, the following recommendations are proposed to enhance IoT security:

1. **Awareness Campaigns:** Launch educational initiatives targeting IoT users to bridge the knowledge gap and promote best practices for securing devices.
2. **Advanced Detection Tools:** Develop and deploy intuitive tools capable of identifying and mitigating DDoS attacks in real-time.
3. **Robust Protocols:** Encourage the adoption of secure IoT communication protocols and regular software updates to minimize vulnerabilities.
4. **Collaborative Efforts:** Foster collaboration between researchers, industry leaders, and governments to establish global standards for IoT security.

- **IDENTIFYING DDoS ATTACK**

A Distributed Denial of Service (DDoS) attack originates by a number of interconnected computers that transmit malicious traffic to a single victim or system. DDoS is harder to track down and faster than a Denial of Service (DoS) assault. It results in problems with availability. On a network, availability and service problems are frequent. Knowing or being able to differentiate between those independent operational problems and DDoS attacks is crucial. Occasionally, a DDoS assault may appear to be normal. In order to identify whether an attack is occurring and to ascertain the attack mechanism, a thorough traffic analysis is required.

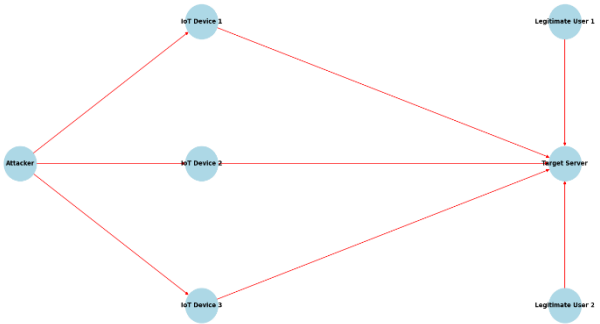
1. The DDoS attack does not have a particular internet protocol (IP) address. It has several IP addresses that make an unlimited request over a short period [4].
2. DDoS attacks are like an unplanned traffic jam jamming up the highway; they completely halt your system from accepting outside traffic, which prevents companies or organizations from providing services to users [5].
3. If the server returns a 503 HTTP error response, it indicates that the server is either overloaded or unavailable for maintenance, which indicates that your server has been compromised by DDoS [4].

There are common signs of DDoS attacks, which we can recognize or observe to assess the attack and take immediate measures for it.

- Poor internet connectivity
- Reduce performance
- Slow access to files
- Incapability to access a specific website[6]
- High demand for a single runner or endpoint.
- Important data and documents crash.
- An inordinate quantum of spam emails [6].
- Logs reveal a robust and well-balanced bandwidth surge.
- Bandwidth should stay the same for a server that operates normally.

- **DDoS ATTACK DETECTION IoT NETWORKS**

In certain situations, DDoS attackers can benefit from the Internet of Things even more than regular users can. Large attack shells are exposed by IoT-connected devices, which also usually pay little attention to security best practices [7]. In rare instances, the authentication credentials might not be updated completely. Devices also many times come without the capability to upgrade repair or increase the software, furthermore exposing them to attacks that exploit well-known vulnerabilities. Massive DDoS attacks are increasingly being launched using IoT botnets. A network of computers with malicious software installed is referred to as a "botnet." [3]. Hackers use this to send space manages without being traced easily. A bot is nothing but software that can be installed in the vulnerable machine to send common to the infected machine to generate traffic and problems.



MESH Protocol: The DDoS detection phase is executed by assigning many amounts of or more service capacity to the server. The service capacity of a server can be defined as the maximum number of requests a server can reuse in a unit of time. also, a service threshold which is a chance that the service capacity is assigned to a server. A DDoS attack is associated when the number of service requests exceeds the maximum service capacity or the service threshold that is assigned to the server. Once a DDoS attack is detected, an ALERT packet is sent to all nodes by the server to make them apprehensive that a DDoS attack is detected. Once an ALERT packet is transferred, all the nodes will enter into an attack identification phase. After the DALERT packet is transferred to the nodes, the nodes will enter into an attack identification phase[8].

DDoS Attacks on LTE Mobile Network: Due to the 4G LTE network is all-IP, mobile operators are susceptible to security attacks, and distributed denial of service attacks are becoming more common on mobile networks. According to this report, DDoS is the biggest security threat to Internet data centers. Research recommends that attackers use the security flaws in the mobile operating system (OS) and apps that are downloaded from the app stores to compromise mobile devices. DDoS attacks against the Long-Term Evolution core network can affect all mobility network data services. A major US cellular operator's Instant Messaging network has an outage due to an app update. The Android application installed on the smartphone kept on checking the central server frequently with many messages into messaging and EPC core[9].

FINDING: There are some prevention techniques to secure your system and network from DDoS attack

1) **Have a DDoS plan:** Having a security assignment plan can assist identify potential threats in your organization's deficiencies and establish a response strategy in case of a DDoS assault [10].
2) **Protect your network:** Install the required tools to safeguard your network infrastructure and applications. Tools such as firewalls, antivirus software, antimalware software, and network monitoring systems can assist you in monitoring network traffic and setting up flood detection alerts [10].
3) **Everything regularly updates:** Update your network and system often to address any issues that may have started. when a DDoS attack occurs. In today's digital world, where there are numerous risks and weaknesses to enjoying the network and current activities, preventing the threat is the only viable alternative because it is very difficult to discover after the assault [10].
4) **Firewall:** This piece of hardware or software is in charge of preventing any incoming or outgoing internet traffic from reaching your computer. Network security requires firewalls. They can be set up to allow a specific amount of traffic or to prohibit particular types of traffic [3].
5) **IDS:** The purpose of an intrusion detection system (IDS) is to identify instances of unapproved system access. It functions in tandem with a router and firewall. Most of the attacks are a distinct signature that causes some concern and highlights that kind of attack most organizations and companies try to develop that kind of signature in a database and store it in the IDS. So, the IDS analyzes incoming traffic and looks at traffic coming in and going out compared to the database of the signature that it has and if it matches any of the signatures it will detect some attack and then send an alert to the administrator. It manually comes in and checks it out[3].
6) **Honeypots:** Honeypots: These are computer networks that invite intruders. It is employed to trick or fool attackers and defend the actual network from intrusions. Honey pots are a decoy system that is created to showcase a sudden set of vulnerabilities to try to attack the attention of an attacker. It is used to deceive the attacker. For example, if the attacker is able to bypass your firewall and your IDS now can scan the entire subnet then scan it. that would come across pretty vulnerable devices or showcase vulnerabilities which it should be in the case of a hacker because they would think that it is a vulnerable server that contains some vulnerable data and that is exactly what honey pot is. A decoy server trying to as a production server or showcase valuable data but also has some vulnerabilities in it. So, that the attacker can be attracted to it and spend some time trying to attack it or analyze Honeypot and the same time honeypot analyzes data traffic and will warn the administrator of possible intrusion we feel that gives time to secure the rest of the network and also get to analyze the logs of the honeypots to try to understand what kind of attacks that attacker trying to create and try to reverse identify at the same time[3].
7) **Use the cloud:** The Cloud has greater bandwidth and resources. It is also to be noted that cloud base apps that observe malicious traffic where before it reaches its intended destination[3].

• CONCLUSION

Distributed Denial of Service (DDoS) Attacks over the IoT networks is implemented in this paper [2]. The DDoS attack uses multiple connected devices that attack a single victim. Understanding the risks, vulnerabilities, and hazards associated with DDoS assaults is crucial because they provide serious economic risks with long-lasting consequences [2]. We discussed the different types of DDoS attacks in IoT networks as well as the motivations behind them[2]. We have discussed the detailed classification of DDoS attacks their consequences of them and also their prevention techniques. Additionally, it will provide signs to recognize a DDoS attack has been reported. after deeply analyzing the different researchers' work, we concluded that the attacker can cause damage to data and decrease the business's reputation attackers, Data tampering is done to spread sedition among people and to incite against each other in politics.

- **REFERENCES**

[1] "How to Prevent DDoS Attacks | Embroker." https://www.embroker.com/blog/how-to-prevent-ddos-attacks/ (accessed Dec. 14, 2022).

[2] A. Irum, M. A. Khan, A. Noor, and B. Shabir, "DDoS Detection and Prevention In the Internet of Things." EasyChair, Jan. 29, 2020.

[3] "Cyber Security Full Course 2022 | Cyber Security Course Training For Beginners 2022 | Simplilearn - YouTube." https://www.youtube.com/watch?v=7vWHYwvFFVY&t=6105s (accessed Dec. 14, 2022).

[4] "What is a DDoS attack? Distributed Denial-of-Service attacks explained." https://www.techtarget.com/searchsecurity/definition/distributed-denial-of-service-attack (accessed Dec. 14, 2022).

[5] "What is a distributed denial-of-service (DDoS) attack? | Cloudflare." https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (accessed Dec. 14, 2022).

[6] "DDoS attacks: A guide + DDoS attack protection tips - Norton." https://us.norton.com/blog/emerging-threats/ddos-attacks (accessed Dec. 14, 2022).

[7] P. Renuka and B. Booba, "Analysis on Detecting DDoS Attack in IoT Environment".

[8] S. E. Anto, S. Seetha, and R. K. Kuriakose, "A Survey on DoS Attacks and Detection Schemes in Wireless Mesh Networks," *Procedia Eng*, vol. 38, pp. 2329–2336, Jan. 2012, doi: 10.1016/J.PROENG.2012.06.278.

[9] J. Henrydoss and T. Boult, "Critical security review and study of DDoS attacks on LTE mobile network," *Proceedings, APWiMob 2014: IEEE Asia Pacific Conference on Wireless and Mobile 2014*, pp. 194–200, Oct. 2014, doi: 10.1109/APWIMOB.2014.6920286.

[10] "Ways to Prevent DDoS Attack | Cyber Chasse - YouTube." https://www.youtube.com/watch?v=E6t_jrk3LUs (accessed Dec. 14, 2022).