ISSN: 0976-0172

Journal of Bioscience And Technology
www.jbstonline.com

# A Framework for Detecting and Mitigating DDoS Attacks in Internet of Things (IoT) Environments

***Dr.A.Janardhan[1]., B.Sravani[2]***

*1 Professor, Department of CSE, Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India*

*2, B.Tech CSE (19RG1A0551), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India*

,

***Article Info***

*Received: 29-12-2020* *Revised: 18-01-2022* *Accepted: 28-01-2022*

## ABSTRACT

***These days, the automotive, home appliance, and industrial sectors, among many other industries, employ a lot of Internet of Things (IoT) devices. The main reason the Internet of Things doesn't draw more users is security concerns. Every day, millions of vulnerabilities that are just waiting to be exploited coexist with new technologies. The Internet of Things is the newest fad, and like any technology, it can be exploited. Distributed Denial of Service (DDoS) attacks have the potential to be a serious problem in Internet of Things environments since conventional IoT devices have limited processing and power capabilities and emphasize providing functionality above security measures. The most frequent kind of assault that may take down a whole network without finding a security flaw in the network is a denial-of-service attack (DDoS). This work's primary goal is to use the Raspberry Pi honeypot concept to prevent DDoS assaults against the Internet of Things. Network configurations containing purposeful flaws are known as honeypots. A honey pot's objective is to attract attackers in order to study their tactics and behaviors and to assist improve network security. After reading through a few research publications, it was determined that although many academics have offered DDoS attack mitigation approaches, relatively few have been recommended for use in IoT environments. The main goal of this dissertation study is to provide low-cost, high-performance DDoS attack mitigation strategies for IoT devices employing honeypots and IDS.***

***Keywords: distributed denial of service attack, internet of things, security breach, and denial of service***

## 1. INDRODUCTION

### 1.1 Internet of things

Given that anything may now be accessible over the Internet, the term "Internet of Things" is no longer used by anybody. The Internet of Things (IoT) is a network of physical objects, cars, and other items integrated with electronics, software, sensors, actuators, and network connection that allow these objects to share and gather data, according to Wikipedia.[1] A person wearing a smart watch, a farm equipped with sensors, a vehicle equipped with built-in sensors alerting the driver to objects nearby, or any other item having an IP address for connecting to a network and transferring data may all be considered "things" in the context of the internet of things.

The term "Internet of Things" (IoT) refers to the broad concept of system devices' capacity to be flexible enough to detect and collect data from the environment around us. This data is then shared via the internet to be processed and utilized for a variety of fascinating reasons. These days, some people refer to the Internet of Things (IoT) as the Industrial Internet instead of IoT.This essentially refers to commercial applications of IoT innovation in the industrial sector.

### 1.2 Dos/DDos Attack

A denial of service (DoS) assault occurs when a service that is normally operable becomes unavailable. Though there are a variety of causes for inaccessibility, it always relates to infrastructure that is overloaded with capabilities and is unable to function properly. An excessive number of systems maliciously assault a single target system or network

ISSN: 0976-0172

Journal of Bioscience And Technology
www.jbstonline.com

during a Distributed Denial of Service (DDoS) attack. This assault is often carried out by a botnet, which is a collection of machines that have been programmed to request a certain service simultaneously.

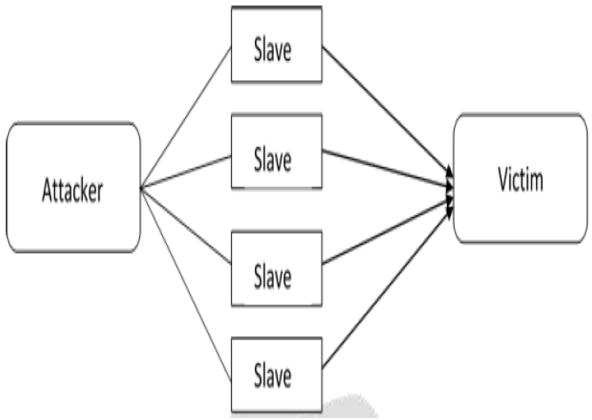



**Fig.1:** DDos Attack flow

Figure 1 depicts the typical course of a DDoS assault, in which the attacker uses slave computers as a botnet to launch attacks such as flooding the victim system with packets to eat up resources and bandwidth on the network. People are becoming used to IoT gadgets these days, such as smart refrigerators, smart phones, and smart watches. As people use more and more IoT in their everyday lives and as the number of devices they own grows daily, IoT assaults are becoming a serious problem. The attacks mentioned above are typical ones that occur in IoT setups. DDoS attacks are particularly dangerous due to their ability to exploit the low processing capability of Internet of Things devices. DDoS assault rendered the gadget unreliable or careless. One thing is certain as we approach 2017: distributed denial-of-service (DDoS) attacks made a splash in 2016. Half-track 124,000 DDoS assaults per week between January 2015 and June 2016 at Arbor Networks. Furthermore, compared to 223 assaults in total in 2015, 274 attacks detected in the first half of 2016 reported at speeds above 100 Gbps, while 46 attacks recorded speeds exceeding 200 Gbps (against 16 in 2015).

When combined, the campaigns' peak assault magnitude increased to 579 Gbps, a 73% increase.

### 1.3 CLASSIFICATION OF DDOS ATTACK

1) ***UDP flood***
***2) ICMP/PING flood***
***3) SYN flood***
***4) Ping of Death***
***5) DNS amplification***

## 2. RELATED WORK

In order to protect enterprises from these assaults, the authors of article [2] provided an equipment-based watermarking checking framework technology. This approach makes use of trace-back techniques to investigate the arriving packets for trust. Only trustworthy packets are allowed within the network during this process. An intrusion detection system that combines a layered model and neural network integration was presented by the authors in article [3]. They specifically suggested two models, A and B, where model A takes into account every characteristic in the practice dataset and model B takes into account features that are added to the order method. The four common attack types identified by this suggested methodology are denial-of-service (DoS), remote to local (R2L), user to root (U2R), and ordinary records. The KDD 1999 database was utilized by this framework with the explicit intention of producing accurate findings. Furthermore, this method has a lower false alarm rate in addition to being able to identify a broad range of threats. A software-defined network-based method for mitigating DDoS attacks is provided in Paper [4]. This article provides a method that is not restricted by router proprietary software. In this article, the author describes a method for detecting anomalies using SDN architecture. This method involves gathering traffic data flow information that is kept up to date on all of the network's SDN-enabled switches. High detection accuracy is successfully achieved with this technology. Future work on efficiently distributing in-line sampling-based ADSs will be necessary to mitigate the impact of increasing IP traffic and constrained computing resources. The author in [5] provides techniques for detecting and mitigating DDoS attacks that are differentiated by different phases. Every step of the DDoS assault has the ability to screen malicious individuals. The phases are referred to as CAPTCHA verification, traffic rate limiting, and user access restriction. Blacklisting IP addresses is a concept used in access restriction. Reducing the pace of http connections limits the same IPs from accessing the same item on the server throughout the rate limitation and Captcha verification stages. The Dendric Cell Algorithm (DCA) is a method that the author presented in article [6] that continuously checks traffic and compares the ratio of SYN packets to SYN-ACK packets. A ratio greater than the median indicates a large volume of incoming SYN packets and a low volume of SYN_ACK packets. In this manner, a TCP SYN

ISSN: 0976-0172

Journal of Bioscience And Technology
www.jbstonline.com

flood attack is found. This suggested system is written in Python and is compatible with IDS systems. The authors of [7] suggest an event detection system that may be integrated into Internet of Things gadgets. The suggested module may identify DDoS assaults by focusing on how the system behaves and using data from the time synchronization service's usage of NTP (Network Time Protocol). The benefit of this solution is that, in contrast to the ones now in use, it doesn't need any costly instruments or equipment (such a monitoring server) or ongoing technical upkeep.

## 3. PROPOSED SYSTEM

According to a study regarding DDoS attack mitigation strategies, as IoT devices have limited processing power, it is not feasible to provide security on every device. Nevertheless, this study is only theoretical at this point, and only theoretical models are being put out. One undiscovered area in IoT systems is the practical use of Rule-based detection and mitigation for DDoS attack avoidance. In light of this, we want to implement a rule-based security system for an Internet of Things setting in this research project. Using a rule-based detection system would assist to both minimize the DDoS assault and gather information about the perpetrator for use in preventing such attacks in the future. Using a rule-based security system on a Raspberry Pi might prove to be an economical option. After reading a few research papers on DDoS detection methods, it seems that using rule-based intrusion detection systems is still a frontier in the Internet of Things. In order to preserve efficiency (data received/transmitted), rule-based security systems that are protected like pillars are used to combat DoS attacks in IoT environments.

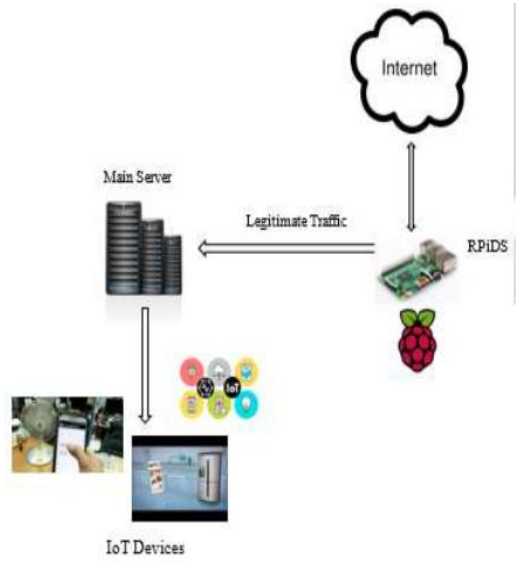



**Fig.2**: Proposed system architecture

### 3.1 Proposed system (Flow Diagram)

Overall flow diagram of the proposed work as shown below. Proposed work divided into two part as detection of the
malicious traffic and mitigation of the DDoS attack.

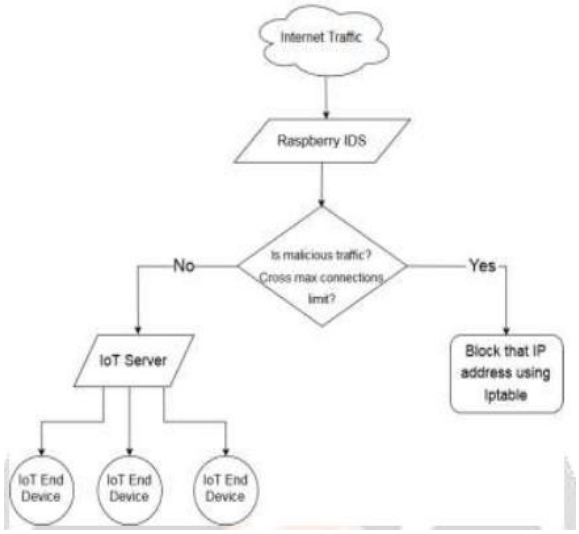



**Fig.3:** Flow diagram

Overall process of the detection and mitigation of DDoS attack following below flow diagram.

ISSN: 0976-0172

Journal of Bioscience And Technology
www.jbstonline.com

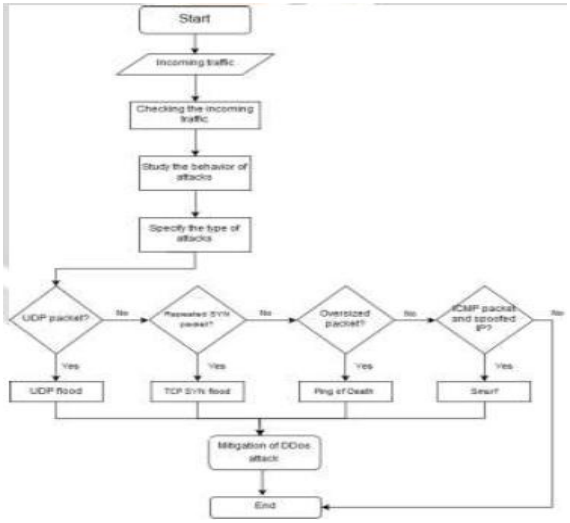



**Fig.4:** DDoS identification Flow chart

The proposed system operates based on the flow diagram shown above. Every time a client makes an online request for an IoT device, RPiDS first checks the request for any unauthorized requests. IP addresses are prohibited by Iptables rules if an intrusion detection system (IDS) detects malicious activity or if the maximum connection limit has been exceeded. Iptables then examines the packet linked to the query. Block that IP address if it detects an ICMP flood, UDP flood, SYN flood, TCP flood, or HTTP flood assault. A Raspberry device running Raspbian OS is called an RPiDS device. It can identify intrusions using rules and mitigate them using Iptables.

## 4. IMPLEMENTATION

This is where the implementation flow would be explained. The three components of implant work are as follows:

Installation: Using a Raspberry Pi device, Raspbian OS Putty, Windows, and Linux OS on 5–6 machines for DDoS attack; Snort IDS in Raspberry PI; DDoS Attack tools in Windows OS; Kali Linux for further assaulting tools.

setup: Snort setup for the Raspberry Pi network interface, SSH connection to the Raspberry Pi using Putty Establish and Define Rules for DoS and DDoS Attack Detection and Establish and Configure Iptables Rules on a Raspberry Pi Network interface, Kali and Windows OS setup tools for attacks Raspberry Pi backup, Set up the test bed. Look for a variety of DDoS attack tools, Put them on machines 5 and 6. Configure the bandwidth based on the test scenario and link every system to the Raspberry Pi network.

Testing: Launch a DDoS assault, Prepare the test report and verify the Raspberry Pi's network bandwidth and resource (memory, cache) monitor. Here are a few screenshots showing how the suggested work is being implemented.

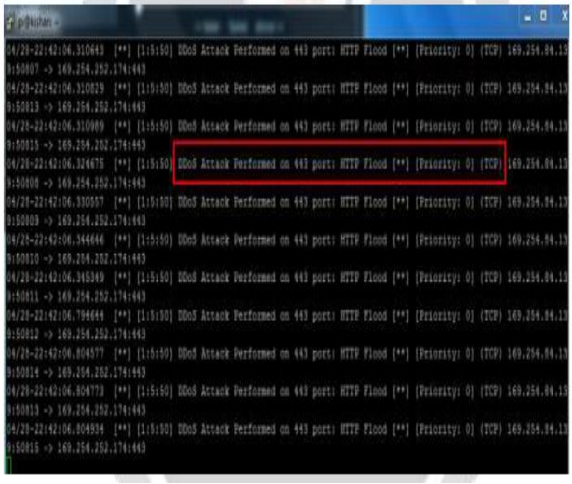


**Fig.6:** Http flood attack detected

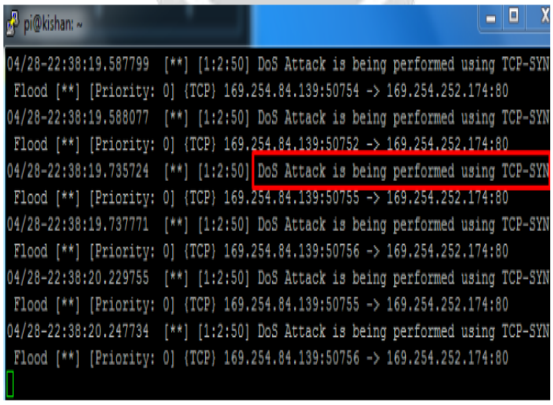
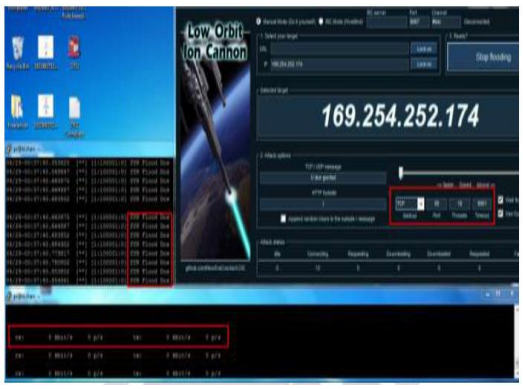



**Fig.7:** TCP-SYN attack detected



ISSN: 0976-0172

Journal of Bioscience And Technology
www.jbstonline.com

**Fig.8:** Mitigation of DDoS attack

## 5. RESULT AND ANALYSIS

This is when the IoT server is subjected to a series of attacks. The suggested system solution effectively detects and mitigates the various DDoS attack types. Below is a list of all the test results. Manual testing is used to test the proposed system. Every assault is carried out twenty times. The graph below illustrates the percentages of detection and mitigation for SYN, TCP, UDP, HTTP, and ICMP flood attacks, which are 100%, 85%, 100%, and 100%, respectively. The suggested task has an overall efficiency of 96% once testing data are analyzed.

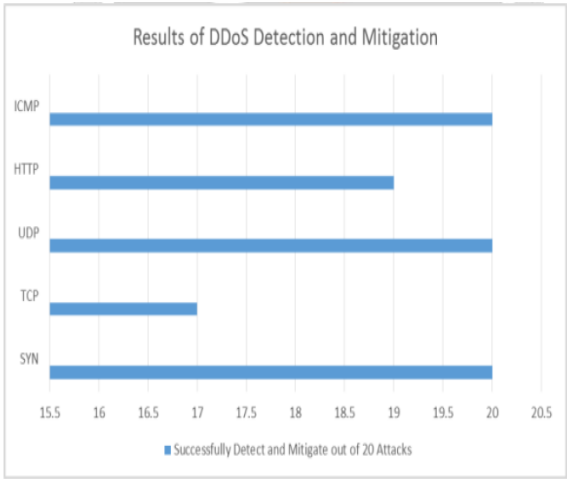



**Chart.1:** Result and Analysis

## 6. CONCLUSIONS

The need to protect the IoT environment against DDoS attacks has arisen with the rise of IoT technologies. The most difficult challenge is identifying DDoS assaults and mitigating them. The suggested system, which is built on a Raspberry Pi, uses a rule-based methodology to identify and mitigate DDoS attacks. The suggested solution accurately recognizes and neutralizes DDoS attacks in Internet of Things environments. This thesis provides a thorough understanding of the Internet of Things, DDoS attacks, and approaches for detecting and mitigating these attacks.

## 7. REFERENCES

*[1] M. Ahmed and H. Kim, "DDoS Attack Mitigation in Internet of Things Using Software Defined Networking",*
*2017 IEEE Third International Conference on Big Data Computing Service and Applications (BigDataService),*
*2017.*
*[2] K. Singh and T. De, "DDOS Attack Detection and Mitigation Technique Based on Http Count and Verification*
*Using CAPTCHA", 2015 International Conference on Computational Intelligence and Networks, 2015.*
*[3] G. Ramadhan, Y. Kurniawan and Chang-Soo Kim, "Design of TCP SYN Flood DDoS attack detection using*
*artificial immune systems", 2016 6th International Conference on System Engineering and Technology (ICSET),*
*2016.*
*[4] T. Kawamura, M. Fukushi, Y. Hirano, Y. Fujita and Y. Hamamoto, "An NTP-based detection module for DDoS*
*attacks on IoT", 2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), 2017.*
*[5] S. Dowling, M. Schukat and H. Melvin, "A ZigBee honeypot to assess IoT cyberattack behaviour", 2017 28th*
*Irish Signals and Systems Conference (ISSC), 2017.*
*[6] S. Misra, P. Krishna, H. Agarwal, A. Saxena and M. Obaidat, "A Learning Automata Based Solution for Preventing Distributed Denial of Service in Internet of Things", 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, 2011.*
*[7] S. Khattab, C. Sangpachatanaruk, D. Mosse, R. Melhem and T. Znati, "Roaming honeypots for mitigating service-level denial-of-service attacks", 24th International Conference on Distributed Computing Systems, 2004.*
*Proceedings, 2004.*