

**Project Report**  
on  
**DDoS Attack Detection and Prevention System**

*Submitted in partial fulfillment of the  
requirement for the award of the degree of*

**Btech CSE**



[Established under Galgotias University Uttar Pradesh Act No. 14 of 2011]

**Under The Supervision of**  
**Name of Supervisor :**  
**Designation**

**Submitted By**

Vaibhav Tyagi  
(20SCSE1010245)

Mayank Singh Yadav  
(20SCSE1010101)

**SCHOOL OF COMPUTING SCIENCE AND ENGINEERING**  
**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**  
**GALGOTIAS UNIVERSITY, GREATER NOIDA**  
**INDIA**  
**MONTH, YEAR**



**SCHOOL OF COMPUTING SCIENCE AND  
ENGINEERING  
GALGOTIAS UNIVERSITY, GREATER NOIDA**

**CANDIDATE'S DECLARATION**

I/We hereby certify that the work which is being presented in the thesis/project/dissertation, entitled **“DDOS ATTACK DETECTION AND PREVENTION SYSTEM”** in partial fulfillment of the requirements for the award of the Btech submitted in the School of Computing Science and Engineering of Galgotias University, Greater Noida, is an original work carried out during the period of month, Aug 2021 to Dec 2021, under the supervision of Ms Indervati Department of Computer Science and Engineering of School of Computing Science and Engineering , Galgotias University, Greater Noida

The matter presented in the Project has not been submitted by us for the award of any other degree of this or any other places.

Vaibhav Tyagi (20SCSE1010245)  
Mayank Singh Yadav (20SCSE1010101)

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

Ms. Indervati

**CERTIFICATE**

The Final Project Viva-Voce examination of Vaibhav Tyagi (20SCSE1010245) and Mayank Singh Yadav (20SCSE1010101) has been held on 23<sup>rd</sup> Dec 2021 and their work is recommended for the award of Btech

**Signature of Examiner(s)**

**Signature of Supervisor(s)**

**Signature of Project Coordinator**

**Signature of Dean**

Date: 23<sup>rd</sup> Dec, 2021

Place: Greater Noida

## **Contents**

<b>Title</b>	<b>Page No.</b>
<b>Candidates Declaration</b>	<b>I</b>
<b>Acknowledgement</b>	<b>II</b>
<b>Abstract</b>	<b>III</b>
<b>Contents</b>	<b>IV</b>
<b>Acronyms</b>	<b>VII</b>
<b>Chapter 1</b>	
<b>Introduction</b>	<b>4</b>
1.1 Problem Identification	<b>5</b>
1.2 Problem Objective	<b>5</b>
1.2.1 Future Scope and Direction	
<b>Chapter 2</b>	
<b>Literature Survey</b>	<b>6</b>
<b>Chapter 3</b>	
<b>Overview</b>	<b>7</b>
<b>Chapter 4</b>	
<b>Working</b>	<b>7-8</b>
<b>Chapter 5</b>	
<b>Conclusion and Future Scope</b>	<b>9</b>
<b>Reference</b>	<b>9</b>
<b>Publication</b>	<b>10</b>

## Acknowledgement

I would like to thank everyone who has contributed to the successful completion of this project. First, I would like to express my utmost gratitude to my research supervisor, Ms. Indervati who in spite of being extraordinarily busy with her duties, took time to give invaluable advice and guidance throughout the development of the research.

In addition, I would also like to express my deepest appreciation to my loving parents and family members for their constant support and encouragement.

Last but not the least, I am grateful for the unselfish cooperation and assistance that my friends had given me to complete this task

## Abstract

**While many offline-based detection approaches have been well studied, the on-line detection of DDoS attack at leaf router near victims still poses quite a challenge to network administrators. Based on per-IP traffic behavioral analysis, this paper presents a real-time DDoS attack detection and prevention system which can be deployed at the leaf router to monitor and detect DDoS attacks. The advantages of this system lie in its statelessness and low computation overhead, which makes the system itself immune to flooding attacks. Based on the synchronization of TCP and UDP protocol behavior, this system periodically samples every single IP user's sending and receiving traffic and judges whether its traffic behavior meets the synchronization or not. A new non-parametric CUSUM algorithm is applied to detect SYN flooding attacks. Moreover, this system can recognize attackers, victims and normal users, and filter or forward IP packets by means of a quick identification technique. Finally, experiment results show that the system can make a real-time detection for flooding attacks at the early attacking stage, and take effective measures to quench it.**

## Introduction

This project is about DDoS attack detection and prevention system. In this Chapter the problem and motivation beside objective and project scope has been covered.

**1.1 Problem Identification-**During past decade, DDoS attacks have posed a powerful security threat to many ISPs, and brought enormous economic losses to them. **In May 2009, hackers induced DDoS attacks towards some of China Telecom's main DNS servers, resulting in the problem that hundreds of websites stopped services.** According to Arbor's survey in 2008, SYN flooding attacks, DNS flooding attacks and Smurf attacks are three main ways of DDoS attacks, and 76% of which are SYN flooding attacks [1].

The major steps of DDoS attacks are shown as follows. Firstly, attackers exploit the technology of client/server, and establish a botnet by combining with multiple vulnerable computers. Secondly,

attackers send commands to the botnet and launch the attack of Denial-of-Service (DoS) for one or several targets. The botnet will increasingly amplify the

power of the DoS attack and make the target consume many system resources. Finally, the victims can not work normally. Based above analysis, DDoS attacks include the following three main characteristics: (1) the quantity of attack source is gigantic but individual attack traffic is little, (2) attacker's traffics often resemble legitimate traffic and (3) the attack patterns will be mixed up to ignite a real attack.

To deal with above problems, this paper put forward a per-IP behavior analysis approach, which is implemented in an online, real-time DDoS attack detection and prevention system. The main contributions of this paper are shown as follows.

(1) Based on per-IP behavioral analysis, a new DDoS detection system is realized. For each IP user, our system will create records for every single IP user's sending and receiving traffic and judge its behavior whether meets the normal principles. Comparing with recording huge number of flows, our approach can greatly reduce the amount of computation and memory consumption.

(2) A specific packet identification technique is utilized to reach real-time flooding attack detection goal. It has improved the system performances dramatically.

(3) A non-parameter CUSUM algorithm is applied to detect the abnormal behavior of each IP. Based on a decision algorithm, each IP user will be classified as attacker, victim or normal user. After differentiate the attacker, the system will block its traffic and forward the normal user packets.

The remainder of this paper is structured as follows. Section II surveys related work. Section III introduces the system architecture. Section IV describes the proposed flooding detection algorithm. Section V evaluates the system and shows its performance results. Section VI concludes the paper.

## **1.2 Project Objective**

In order to solve the drawbacks of the previous system stated in 1.1, the existing system will need to evolve. The proposed system will reduce the paperwork where DDoS attack will no longer take place, moreover if took place doesn't damage the server or the individual system. The new system will also reduce Chances of fatal errors and crashing due to attacks.

## **1.2 Project Scope and Direction**

The main intention of this project is to solve the issues of system failure due to DDoS attacks while reproducing a brand new innovative smart system that can provide convenience to the server admins. In this project, an application will be developed which is capable of recognising the attack and preventing it so that server remain protected from crashing or failure.

### **The followings are the project scopes:**

- The targeted servers are analysed and check for traffic overflow
- The Server in case of traffic overflow should be slowed down by introducing captcha

- Server having sensitive data should be protected with passwords
- The device on which attack took place will be slowed and being analysed for traffic overloader IP

## Literature

### **2.1 Denial-of-Service (DoS) Attack and Botnet: Network Analysis, Research Tactics, and Mitigation**

This describes how the consequence and hazards showcased by Denial of Service attacks have resulted in the surge of research studies, commercial software and innovative cogitations. Of the DoS attacks, the incursion of its variant DDoS can be quite severe. A botnet, on the other hand, is a group of hijacked devices that are connected by internet. These botnet servers are used to perform DDoS attacks effectively. In this chapter, the authors attempt to provide an insight into DoS attacks and botnets, focusing on their analysis and mitigation. They also propose a defense mechanism to mitigate our system from botnet DDoS attacks. This is achieved by using a through access list based configuration. The artful engineering of malware is a weapon used for online crime and the ideas behind it are profit-motivated. The last section of the chapter provides an understanding of the WannaCry Ransomware Attack which locked computers in more than 150 countries.

### **2.2 A study on IDS for preventing Denial of Service attack using outliers techniques**

Denial of service attack permits the intruders to access the network services thereby preventing the legitimate users to access the services. To overcome the deficits of the DoS attack, it is very essential to design an intrusion detection system. Intrusion detection system (IDS) is software that operates as a network security mechanism to protect the computer network system from attacks. With increasing number of data being transmitted gradually from one network to another, the IDS identify the intrusions in such large datasets effectively. Data mining is an efficient tool applied to outline the intrusion detection system and prevent the massive network data from the intruders. Outliers are patterns in data that do not match to a well-defined notion of normal behavior. Outlier detection aims to find patterns in data that do not conform to expected behavior. It is widely used for developing intrusion detection in cyber security. This paper presents the study of outlier detection technique and how it is used to develop the intrusion detection system to overcome the DOS attack.

### **2.3 Research about DoS Attack against ICPS**

This paper studies denial-of-services (DoS) attacks against industrial cyber-physical systems (ICPSs) for which we built a proper ICPS model and attack model. According to the impact of different attack rates on systems, instead of directly studying the time delay caused by the attacks some security zones are identified, which display how a DoS attack destroys the stable status of the ICPS. Research on security zone division is consistent with the fact that ICPSs' communication devices actually have some capacity for large network traffic. The research on DoS attacks' impacts on ICPSs by studying their operation conditions in different security zones is simplified further. Then, a detection method and a mimicry security switch strategy are proposed to defend against malicious DoS attacks and bring the ICPS under

attack back to normal. Lastly, practical implementation experiments have been carried out to illustrate the effectiveness and efficiency of the method we propose.

## Overview

The proposed system is a software system which help to identify DDoS attack or traffic overloading. This system includes a script that gets triggered when the traffic increases exponentially. This script will Slow down the website traffic hence preventing the attack

### Steps of Working:

- - Setting a condition if traffic crosses a certain number
- - as the traffic hits the target which inturn triggers the python script that enable a html code which direct the user to a captcha page
- - User then need to solve captcha
- - Due to captcha solving the traffic slows down.
- - Captcha solving give the server time to cool down and meet the new traffic

## Working

### Code

#### Python Script To trigger Captcha

```
import webbrowser
import os

# to open/create a new html file in the write mode
f = open('Captcha.html', 'w')

# the html code which will go in the file Captcha.html
html_template = """

<html>
<head></head>
<body>
<p><!-- START CAPTCHA -->
<br>
<div class="capbox">

<div id="CaptchaDiv"></div>

<div class="capbox-inner">
Type the number:<br>
```

```

<input type="hidden" id="txtCaptcha">
<input type="text" name="CaptchaInput" id="CaptchaInput" size="15"><br>

</div>
</div>
<br><br>
<!-- END CAPTCHA --></p>

</body>
</html>
"""
# writing the code into the file
f.write(html_template)

# close the file
f.close()

# 1st method how to open html files in chrome using
filename = 'file:///'+os.getcwd()+ '/' + 'GFG.html'
webbrowser.open_new_tab(filename)

```

## Javascript For Captcha Validation

```

<script type="text/javascript">

// Captcha Script

function checkform(theform){
var why = "";

if(theform.CaptchaInput.value == ""){
why += "- Please Enter CAPTCHA Code.\n";
}
if(theform.CaptchaInput.value != ""){
if(ValidCaptcha(theform.CaptchaInput.value) == false){
why += "- The CAPTCHA Code Does Not Match.\n";
}
}
if(why != ""){
alert(why);
return false;
}
}

var a = Math.ceil(Math.random() * 9)+ '';
var b = Math.ceil(Math.random() * 9)+ '';
var c = Math.ceil(Math.random() * 9)+ '';
var d = Math.ceil(Math.random() * 9)+ '';
var e = Math.ceil(Math.random() * 9)+ '';

var code = a + b + c + d + e;
document.getElementById("txtCaptcha").value = code;
document.getElementById("CaptchaDiv").innerHTML = code;

```



```

// Validate input against the generated number
function ValidCaptcha(){
var str1 = removeSpaces(document.getElementById('txtCaptcha').value);
var str2 = removeSpaces(document.getElementById('CaptchaInput').value);
if (str1 == str2){
return true;
}else{
return false;
}
}

// Remove the spaces from the entered and generated code
function removeSpaces(string){
return string.split(' ').join('');
}
</script>

```

## Conclusion

Based on analyzing per-IP traffic behavior approach, a real-time DDoS attack detection and prevention system is realized. It has three advantages shown as follows. 1) Based on per-IP traffic behavior analyses, it is easier to differentiate the attackers from the normal users. 2) Because our approach needs less computation and memory, the system could be deployed for on-line DDoS detection and prevention. 3) By applying the non-parameter CUSUM algorithm and decision algorithm, this system can detect attacks accurately at the earlier attack stage. Moreover, our system can quickly filter the attack traffics and forward the normal traffics simultaneously by means of the fast identification technology. On a campus network, to investigate our system, many tests have been done. The results show that the system has high DDoS detection accuracy and short detection time.

Besides for SYN flooding attacks detection, the system can be utilized to detect DNS flooding attacks and Smurf attacks. That means our system has a wider applying field.

## Reference

1. [1] Arbor Networks. Worldwide Infrastructure Security Report, <http://www.arbornetworks.com/report>, Sept 2008.
2. [2] T. Peng, C. Leckie and R. Kotagiri, "Survey of network-based defense mechanisms countering the DoS and DDoS problems", ACM Comput. Surv. 39, April 2007.
3. [3] R. Sommer and V. Paxson, "Enhancing byte-level network intrusion detection signatures with context", CCS, 2003.
4. [4] X. Li, F. Bian, M. Crovella, C. Diot, R. Govindan, G. Iannaccone and A. Lakhina, "Detection and identification of network anomalies using sketch subspaces", IMC, 2006.
5. [5] H. Ringerg, A. Soule, J. Rexford and C. Diot, "Sensitivity of pca for traffic anomaly detection", SIGMETRICS, 2007.
6. [6] Hemant Sengar, Xinyuan Wang, Haining Wang, Duminda Wijesekera and Sushil Jajodia, "Online Detection of Network Traffic Anomalies Using Behavioral Distance", IEEE IWQoS 2009 , Charleston, July 2009.

# Publication

23/12/2021, 11:41

Gmail - Feedback via the Online Submission - [CS] - Paper ID -I0177909



Vaibhav Tyagi <vaibhavtyagi121001@gmail.com>

---

## Feedback via the Online Submission - [CS] - Paper ID -I0177909

1 message

---

**IJSER Research Publication** <ijser.editor@ijser.org>  
To: vaibhavtyagi121001@gmail.com  
Cc: ijser.editor@gmail.com

Thu, Dec 23, 2021 at 11:29 AM

Dear Author,


Thanks for contacting IJSER !  
We have successfully received your paper.

**Paper Title:** DDoS Attack Prevention System  
**Author\*:** Vaibhav Tyagi , Mayank Singh Yadav  
**Email\*:** [vaibhavtyagi121001@gmail.com](mailto:vaibhavtyagi121001@gmail.com)  
**Abstract\*:** DDoS Attack Prevention system is a python script works on SDN environments. It analyzes the characteristics of traffic flows up-streaming to a Vietnamese ISP server, during both states of normal and DDoS attack traffic. Based on the traffic analysis, an SDN-based Attack Prevention Architecture is proposed that is able to capture and analyze incoming flows on-the-fly. A multi-criteria based Prevention mechanism is then designed using both hard-decision thresholds and Fuzzy Inference System to detect DDoS attack. In response to determining the presence of attacks, the designed system is capable of dropping attacks flows, demanding from the control plane.  
**Attach Research Paper\*:** DDoS Attack Detection and Prevention System.docx  
**Country\*:** India

The result of peer review will be mailed to you once the review process complete.  
For any future communication, kindly refer your Paper ID - I0177909.

Best Regards,  
Editorial Assistant, IJSER  
<http://www.ijser.org>

---

 **Register for IJSER Research Forum** *Create your own thread for research topic of your interest, discuss your research paper with the world leaders., get more citations for your research.*

---

**IJSER Xplore**  **Research Paper Database** - Now search research papers by author name, paper title, keywords.

---