Date: 30 / 03 / 2019

CERTIFICATE

This is to certify that the project dissertation titled “**DETECTION CUM PREVENTION OF DOS/DDOS ATTACK**” being submitted by

1. AFREEN FATIMA (1604-15-733-016)
2. FATEMA HUSSAIN (1604-15-733019)

in Partial Fulfillment of the requirements for the award of the degree of BACHELOR OF ENGINEERING IN COMPUTER SCIENCE AND ENGINEERING in MUFFAKHAM JAH COLLEGE OF ENGINEERING AND TECHNOLOGY, Hyderabad for the academic year 2018-19 is the bonafide work carried out by them. The results embodied in this report have not been submitted to any other University or Institute for the award of any degree or diploma.

Signatures:

Internal Project Guide	Head CSED
(Mrs. Maniza Hijab)	(Dr. A.A. Moiz Qyser)
(Associate Professor)	

External Examiner

DECLARATION

This is to certify that the work reported in the major project entitled "**DETECTION CUM PREVENTION OF DOS/DDOS ATTACK**" is a record of the bonafide work done by us in the Department of Computer Science and Engineering, Muffakham Jah College of Engineering and Technology, Osmania University. The results embodied in this report are based on the project work done entirely by us and not copied from any other source.

1. Afreen Fatima (1604-15-733-016)
2. Fatema Hussain (1604-15-733-019)

ACKNOWLEDGEMENT

Our hearts are filled with gratitude to the Almighty for empowering us with courage, wisdom and strength to complete this project successfully. We give him all the glory, honor and praise.

We thank our Parents for having sacrificed a lot in their lives to impart the best education to us and make us promising professionals for tomorrow.

We would like to express our sincere gratitude and indebtness to our project supervisor **Mrs. Maniza Hijab** for her valuable suggestions and interest throughout the course of this project.

We are happy to express our profound sense of gratitude and indebtedness to **Prof. Dr. Ahmed Abdul Moiz Qyser,** Head of the Computer Science and Engineering Department, for his valuable and intellectual suggestions apart from educate guidance constant encouragement right throughout our work and making successful.

With a great sense of pleasure and privilege, we extend our gratitude to **Prof. Dr. Syed Shabbeer Ahmed,** Associated Head of Computer Science and Engineering Department, project in-charge, offered valuable suggestions was a pre-requisite to carry out support in every step.

We are pleased to acknowledge our indebtedness to all those who devoted themselves directly or indirectly to make this project work a total success.

AFREEN FATIMA

FATEMA HUSSAIN

ABSTRACT

The Denial of Service (DOS) attack is an explicit attempt by an attacker to prevent the legitimate users not to access the services. When this attack is made on a large scale that is by using multiple computers then it’s known as Distributed Denial of Service (DDoS) Attack. An attacker can use many techniques for denial of service like flooding technique which floods a network and reduces the legitimate user bandwidths and thus disrupts the services for the users. In DDoS attack, the attacker tries to interrupt the services of a server and utilizes its CPU and network bandwidth. Flooding DDOS attack is based on a huge volume of attack traffic (e.g. ICMP FLOOD) which is termed as a Flooding based DDOS attack. Flooding-based DDOS attack attempts to congest the victim's network bandwidth with real-looking but unwanted IP data, due to which the legitimate IP packets cannot reach the victim because of lack of bandwidth resource. ICMP FLOOD is used for sending a large number of ICMP packets to a remote host which consumes the victimized system’s resources and eventually causes the system to be unreachable by other clients. In this project firstly, we detect the ICMP Flood by using various methods and tools and then find out the prevention technique for DDOS attack.

Normally, PING requests are used to test the connectivity of two computers by measuring the round-trip time from when an ICMP echo request is sent to and when an ICMP echo reply is received. During an attack, however, they are used to overload a target network with data packets. In order for a PING flood to be sustained, the attacking computer must have access to more bandwidth than the victim. This limits the ability to carry out a DoS attack, especially against a large network.

Additionally, a Distributed Denial of Service (DDoS) attack executed with the use of a botnet has a much greater chance of sustaining a ping flood and overwhelming a target’s resources.

In our project we have proposed a solution which enhances server abilities through traffic pattern observation and attack detection before the attack occurs and taking adaptive measure of banning the attacker IP and thus preventing DDoS PING flooding attack.

CONTENTS

LIST OF FIGURES

LIST OF TABLES