JAIN UNIVERSITY
Declared as Deemed-to-be University u/s 3 of the UGC Act 1956

A Project Report on

DDOS ATTACK USING IOT DEVICE

Submitted by

GAYATHRI SEETHARAM

USN: 16MCAL2012

in partial fulfillment of the 5th Semester

Of

MASTER OF COMPUTER APPLICATIONS

(Specialization - Information Security Management Services)

DEPARTMENT OF COMPUTER SCIENCE & IT

JAIN UNIVERSITY

BANGALORE- 560069.

DECEMBER- 2017

JAIN UNIVERSITY
Declared as Deemed-to-be University u/s 3 of the UGC Act 1956

DEPARTMENT OF COMPUTER SCIENCE & IT

JAIN UNIVERSITY

BANGALORE- 560069

PROJECT WORK DECEMBER 2017

This is to certify that the project entitled

DDOS ATTACK USING IOT DEVICE

is the bonafide record of project work done by

GAYATHRI SEETHARAM

USN :16MCAL2012

during 5th semester MCA(July 2017 - December 2018)

Project Guide

Name : Prof. Parul Pandey

HOD MCA

Dr. S. Jagannathan

Head

Department of Computer Science & IT

Prof. Achutha V

JAIN UNIVERSITY
Declared as Deemed-to-be University u/s 3 of the UGC Act 1956

Department of MCA

CERTIFICATE

This is to certify that the project work entitled **"DDOS ATTACK USING IOT DEVICE"** is a bonafide work carried out by **GAYATHRI SEETHARAM (16MCAL2012),** in partial fulfillment of 5th semester of **Master of Computer Applications (Specialization - Information Security Management Services)**, **Jain University, Bangalore** during the 5th Semester. The project report has been approved as it satisfies the academic requirements in respect of the project work prescribed by Jain University in partial fulfillment of 5th Semester of Master of Computer Applications.

Internal Guide **External Guide**

Head – Department of Computer Science & IT

Name of the Examiners	**Signature with Date**
1)……	**……..**
2)……	**……**

DECLARATION

I affirm that the project work titled "DDOS ATTACK USING IOT DEVICE" being submitted in partial fulfillment of 5th Semester of MCA Specialization - Information Security Management Services is the original work carried out by me. It has not formed the part of any other project work submitted for award of any degree or diploma, either in this or any other University.

Name of the Student: Gayathri Seetharam
USN: 16MCAL2012

ACKNOWLEDGEMENT

It is not the completion of the project that is most important but more so, the interaction of roles played by various people in the satisfactory completion. I take this opportunity to express my deep gratitude and appreciation of all those who encouraged me to successfully complete the project.

With profound sense of gratitude and regards, I acknowledge with great pleasure the guidance and support extended **by**, I thank **Dr. EshwaranIyer,** Dean, Jain Knowledge Campus, Bangalore, **Dr. B.A Vasu,** Center Head, Jain Knowledge Campus Bangalore, **Prof. Achutha V,** Head, Department of Computer science& IT, **Dr. S. Jagannathan**, Head, Master of Computer Applications, Jain University, Bangalore for their interest & encouragement throughout the project

I would like to express my deep sense of gratitude to my Guide Ms.**Parul Pandey, Assistant Porfessor, Department of MCA, Jain University, Bangalore**for her accomplishment and valuable information, direction and sense of perfection to work. She had been main source of inspiration for completion of work and strengthening confidence.

I would also thank my parents for their understanding & encouragement, Department Staffs, teaching and non-teaching, my friends, one and all those who helped me to complete this project successfully

STUDENT NAME: Gayathri Seetharam

USN: 16MCAL2012

ABSTRACT

IoT botnets have been used to launch high-profile DDoS attacks. IoT devices are attractive to attackers because so many of these devices are shipped with insecure defaults, including default administrative credentials, open access to management systems via the Internet-facing interfaces on these devices, and shipping with insecure, remotely exploitable code. A large proportion of embedded systems are rarely if ever updated in order to patch against security vulnerabilities– indeed, many vendors of such devices do not provide security updates at all.

The main aim of this research paper is show how a DDoS attack is launched using IoT. In this, we will be using Mirai malware to infect the IoT devices. The Mirai malware will scan for IP address on the internet and fid vulnerable devices with default credentials and perform a brute force attack on the vulnerable devices and gaining its credentials to infect the devices with Mirai malware.

After performing this attack the command and control will give a command to launch an attack on the specified target. In this project we will have one command and control server which is written in Go programming language, and botnets which is written in c programming language.

TABLE OF CONTENTS