**DETECTION OF DDOS ATTACK IN APPLICATION LAYER BY THE ANALYSIS OF USER BEHAVIOR**

A PROJECT REPORT

***Submitted by***

BL.EN.U4CSE12504 ATHIRA S N

BL.EN.U4CSE12109 SUDHEEKSHA G

BL.EN.U4CSE12105 SRIKANTA B U

***In partial fulfillment for the award of the degree***

***Of***

**BACHELOR OF TECHNOLOGY**

IN

COMPUTER SCIENCE ENGINEERING



AMRITA SCHOOL OF ENGINEERING, BANGALORE

AMRITA VISHWA VIDYAPEETHAM

**BANGALORE 560 035**

**AMRITA VISHWA VIDYAPEETHAM**

**AMRITA SCHOOL OF ENGINEERING, BANGALORE, 560035**



**BONAFIDE CERTIFICATE**

This is to certify that the project report entitled “**DETECTION OF DDOS ATTACK IN APPLICATION LAYER BY THE ANALYSIS OF USER BEHAVIOR”** submitted by:-

BL.EN.U4CSE12504 ATHIRA S N

BL.EN.U4CSE12109 SUDHEEKSHA G

BL.EN.U4CSE12105 SRIKANTA B U

in partial fulfillment of the requirements for the award of the **Degree Bachelor of Technology** in “**COMPUTER SCIENCE AND ENGINEERING**” is a bonafide record of the work carried out under my guidance and supervision at Amrita School of Engineering, Bangalore.

Mrs. Kavitha C. R. Dr. T. S. B. Sudarshan

Asst. Professor Chairperson

Department of CSE Department of CSE

This project report was evaluated by us on ………

INTERNAL EXAMINER EXTERNAL EXAMINER

**ACKNOWLEDGEMENT**

OM AMRITESHWARYAI NAMAHA

No work can be completed without the help from others. Upon satisfactory completion of the project, we would like to thank everyone who has helped us throughout the course o the work.

We would like to take this opportunity to thank Sadhguru Mata Amritanandamayi, the Chancellor of Amrita Vishwa Vidhyapeetham, who has been a driving force, leading to the successful and timely completion of our project. We also thank her for her sustained blessings on us.

We are deeply indebted to Dr. Rakesh S. G., Dean, Amrita School of Engineering, Bangalore, and Dr. T S B Sudharshan, Chairperson, Department if CSE, Amrita School of Engineering, Bangalore who have given us this opportunity ti carry out this project.

Further, we would like to thank our project guide and mentor, Ms. Kavitha C R, who has been with us at every step of this project. We would also like to express our heartfelt gratitude to Dr. Sangeetha Iyer and Ms. Santhana Lakshmi S. who have helped us through some obstacles we faced during the course of the work.

Lastly, we would like to say that our families and friends have always been pillars of strength and have supported us in all ways possible. We would like to express our deepest gratitude to them.

**ABSTRACT**

Distributed denial of service attack is one of the major security threats that is faced in web security. An attacker can attack either using malicious code on normal user machine or by finding a back door to send HTTP traffic. Using statistical pattern recognition application layer DDoS attacks can be recognized.

Steps Involved:

1. From web server log, application layer dataset is constructed.

2. Two types of application layer dataset are taken (Attack and Normal) with instances like Timestamp, URL, Response code, Number of bytes sent etc.

3. Additional features will be constructed to detect the attacks better such as Average number of requests per unit time, Session duration etc.

4. Select effective parameters using PCA (Principle of component analysis)

5. Analysis Report and conclusion about attacks

**TABLE OF CONTENTS**

**DESCRIPTION PAGE NO.**

ACKNOWLEDGEMENT i

ABSTRACT ii

TABLE OF CONTENTS iii

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION 1

1.1 DENIAL OF SERVICE 1

1.1.1 SYMPTOMS 1

1.2 DISTRIBUTED DoS 2

1.3 HOW DDoS ATTACKS WORK 4

1.4 DIFFERENCE B/W DoS AND DDoS 5

1.5 MOTIVATION FOR DDoS ATTACK 6

1.6 TYPES OF DDoS ATTACKS 8

1.6.1 VOLUMETRIC ATTACKS 8

1.6.2 APPLICATION LAYER ATTACKS 10

* + 1. STATE EXHAUSTION ATTACKS 11
    2. SOME MORE SPECIFIC TYPES OF

DDOS ATTACKS 12

1.7 WHY DDoS ATTACKS ARE DANGEROUS 14

1.8 PREPARING FOR DDoS ATTACKS 14

1.9 CONSEQUENCES OF DDoS ATTACKS 15

1.10 DDoS PROTECTION OPTIONS 15

1.10.1 APPLICATION FRONT END H/W 15

1.10.2 APPLICATION LEVEL KEY

COMPLETION INDICATOR 16

1.10.3 BLACKHOLING AND SINKHOLDING 16

1.10.4 DDS BASED DEFENCE 16

1.10.5 FIREWALLS 16

1.10.6 IPS BASED PREVENTION 17

1.10.7 ROUTERS 17

1.10.8 SWITCHES 17

1.10.9 UPSTREAM FILTERING 18

1.11 ABROR’S APPROACH 18

1.12 PROPOSED METHOD 19

2. SOFTWARE REQUIREMENTS SPECIFICATION 20

2.1 REQUIREMENTS 20

2.1.1 CAPABILITY 20

2.1.2 CAPACITY 20

2.1.3 RELIABILITY 20

3. DETAILED DESIGN 21

3.1 INTRODUCTION 21

3.2 LOGICAL DESIGN 21

3.3 HIGH LEVEL DESIGN 21

3.4 LOW LEVEL DESIGN 23

4. IMPLEMENTATION 27

4.1 PREPARING DUMMY DATASET 27

4.2 DATASET PREPROCESSING 27

4.2.1 FEATURE EXTRACTION 27

4.2.2 FEATURE CONSTRUCTION 28

4.3 METHODOLOGY 29

4.3.1 PRINCIPLE COMPONENT ANALYSIS 29

4.3.2 LOGISTIC REGRESSION 32

4.4 ALGORITHM 33

4.4.1 TRAINING DATA SET ALGORITHM 33

4.4.2 TESTING DATA SET ALGORITHM 34

4.5 LANGUAGE AND TOOLS 34

4.5.1 LANGUAGE USED: PYTHON 34

4.5.2 LIBRARIES USED 34

5. TESTING 35

5.1 TESTING METHOD 35

5.1.1 TEST DATA PREPROCESSING 35

5.1.2 TEST PCA 37

5.1.3 TEST LOGISTIC REGRESSION 38

6. CONCLUSION 39

7. FURTURE ENHANCEMENTS 40

8. REFERENCES 41

9. APPENDIX 43