ABSTRACT:

This aids in refining any organization's security policy due to identification of vulnerabilities, and guarantees that the security measures taken actually gives the protection that the organization expects and requires. Administrator needs to perform vulnerability which helps them to uncover shortcomings of network security that can lead to device or information being compromised or destroyed by exploits. These outputs are typically heterogeneous which makes the further analysis a challenging task. Normal user network may give the way to unauthorized people to access as a authorized agents. Whenever, users step into online networks, without knowing them third party or any other harmful person monitoring their behavior. Provide the protection from malicious activity, admin or authorized person also check the user networks such as IP address and email.

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	5
	LIST OF ABBREVIATIONS	10
1.	**CHAPTER 1 : INTRODUCTION** 1.1 INTRODUCTION 1.2 EXISTING SYSTEM 1.2.1 DEMERITS 1.3 LITERATUTRE SURVEY 1.4.PROPOSED SYSTEM 1.4.1 ADVANTAGE	11
2.	**CHAPTER 2 :PROJECT DESCRIPTION** 2.1 METHODOLOGY 2.2 MODULES 2.3 MODULE EXPLANATION 2.4 MODULE DIAGRAM	19

3.	**CHAPTER 3 : REQUIREMENTS ENGINEERING** 3.1 GENERAL 3.2 HARDWARE REQUIREMENTS 3.3 SOFTWARE REQUIREMENTS	23
4.	**CHAPTER 4 : SYSTEM DESIGN ENGINEERING** **4.1 GENERAL** 4.1.1 USE CASE DIAGRAM 4.1.2 ACTIVITY DIAGRAM 4.1.3 DATA FLOW DIAGRAM 4.1.4 ER- ARCHITECTURE 4.1.5 SYSTEM DIAGRAM	25

5.	**CHAPTER 5 :DEVELOPMENT TOOLS** 5.1 GENERAL FRONT END 5.2 FEATURES OF JAVA 5.2.1 THE JAVA FRAMEWORK 5.2.2 OBJECTIVE OF JAVA 5.2.3 JAVA SERVER PAGES-AN OVERVIEW 5.2.4 EVOLUTION OF WEB APPLICATIONS 5.2.5 BENEFITSOF JSP 5.3 SERVLETS 5.4 JAVA SERVLETS 5.5 CONCLUSION	32
7.	**CHAPTER 6 : SNAPSHOTS** 7.1 GENERAL 7.2 VARIOUS SNAPSHOTS	41

8	**CHAPTER 7:** APPLICATIONS AND FUTURE ENHANCEMENT 8.1 FUTURE ENHANCEMENT CONCLUSION REFERENCE	47

LIST OF ABBREVATION

S.NO	ABBREVATION	EXPANSION
1.	DB	DataBase
2.	SMC	Secure MultipartyComputation
3.	MDA	Medical Admin
4.	DBC	Data Base Confidentiality
10	JVM	Java Virtual Machine
11.	JSP	Java Server Page

CHAPTER 1

1.1 INTRODUCTION:

In this paper, we explore how a network can manipulate this information source-the peering link where traffic ingresses a network-to more precisely locate sources of spoofed traffic. Our key observation is that the routes are partially under an origin network's control, and so the network receiving the spoofed traffic has some ability to impact on which link it receives traffic, instead of relying on routers that are not under its control. We propose techniques that are fundamentally Different from existing trace back approaches and can be used today, requiring no changes to deployed equipment nor cooperation from other networks. Our techniques work best when the spoofed traffic originates from few sources, as is common in amplification DoS attacks.

1.2 EXISTING SYSTEM:

CONCEPT:

Network can use to systematically vary BGP announcement configurations to induce changes to Internet routes and to the set of sources routed to each peering link.

1.2.1 Disadvantage:

This scheme cannot be used to detect loops

1.3 LITERATURE SURVEY:

TITLE: LIFEGUARD: Practical Repair of Persistent Route Failures.

AUTHOR: Ethan Katz-Bassett,Colin Scott,David R. Choffnes

YEAR: 2012

PAPER EXPLANATION:

The Internet was designed to always find a route if there is a policy compliant path. However, in many cases, connectivity is disrupted despite the existence of an underlying valid path. The research community has focused on short-term outages that occur during route convergence. There has been less progress on addressing
Avoidable long-lasting outages. Our measurements show that long lasting events contribute significantly to overall unavailability. To address these problems, we develop LIFEGUARD, a system for automatic failure localization and remediation. LIFEGUARD uses active measurements and a historical path atlas to locate faults, even in the presence of asymmetric paths and failures. Given the ability to locate faults, we argue that the Internet protocols should allow edge ISPs to steer traffic to them around failures, without requiring the involvement of the network causing the failure. Although the Internet does not explicitly support this functionality today, we show how to approximate it using carefully crafted BGP messages. LIFEGUARD employs a set of techniques to reroute around failures with low

impact on working routes. Deploying LIFEGUARD on the Internet, we find that it can effectively route traffic around an AS without causing widespread disruption.

TITLE: A survey of distributed denial-of-service attack, prevention, and mitigation techniques

AUTHOR: Tasnuva Mahjabin, Yang Xiao, Guang Sun and Wangdong Jiang.

YEAR: 2017

PAPER EXPLANATION:

Distributed denial-of-service is one kind of the most highlighted and most important attacks of today's cyber world. With simple but extremely powerful attack mechanisms, it introduces an immense threat to current Internet community. In this article, we present a comprehensive survey of distributed denial-of-service attack, prevention, and mitigation techniques. We provide a systematic analysis of this type of attacks including motivations and evolution, analysis of different attacks so far, protection techniques and mitigation techniques, and possible limitations and challenges of existing research. Finally, some important research directions are outlined which require more attentions in near future to ensure successful defense against distributed denial-of-service attacks.

TITLE: Towards Measuring Global DDoS Attack Capacity

AUTHOR: T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Visky

YEAR: 2019

PAPER EXPLANATION:

In today's Internet, distributed denial-of-service (DDoS) attacks play an ever-increasing role and constitute a risk to any commercial, military or governmental
entity that has a presence on the Internet or simply has an Internet connection. To address this threat on all levels, decision-makers have to rely on trustworthy information regarding attack capacity, sources, and the largest contributors. The lack
of this information limits the ability of technicians, policymakers, and other relevant
decision-makers to remediate the issue as efficiently as possible. This research introduces a methodology for measuring the properties of individual devices participating in such attacks. These properties include rate limiting, amplification factor, and speed, which allows the calculation of each device's actual contribution to the attack capacity. This methodology was implemented as a proof of concept for the NTP protocol and the results indicate that it has promising potential.