**ABSTRACT**

This project main aim is to handle thousands of requests (traffic load) on a web portal when millions of users want to access the same webpage. When the user hits on a certain URL and if the requests are more on that URL the traffic load will be more. There will be lagging of the site and can’t be accessed by all the users at a time, to avoid this problem we are going to change the existing policies in AWS Cloud, and create virtual instance servers by using AWS.

The main objective of this project is to maintain auto-scaling and load balancing on a certain web portal. In Load Balancers, Elastic Load Balancing automatically distributes your incoming traffic across multiple targets, such as EC2 instances. Auto-scaling monitors your applications and automatically adjusts capacity to maintain steady and better performance at the lowest cost. Network security consists of the policies and practices to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

Network security consists of the policies and practices to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Only Network security can protect you from Trojan horse viruses. Network security involves the authorization of access to data in a system, controlled by the network administrator. To avoid ARP SPOOFING, MAC FLOODING, and DHCP SPOOFING, we implement security policies. Firewall plays a preeminent role in network security. To prevent unauthorized access, we are using Cisco advanced security appliances. To connect different branches with security, we are implementing SITE TO SITE VPN. To overcome the network attacks, we are developing the Intrusion Prevention System. Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection feature that effectively mitigates a wide range of network attacks. These network security infrastructure is implementing in On-premises, not in a cloud

**ACKNOWLEDGMENT**

We feel thankful to our **P Bala Srinivas** Sir of Aditya College Of Engineering, for his cooperation and help in the completion of our project and throughout our course.

We avail this opportunity to express our heartfelt thanks to our HOD VV Satya Narayana Sir and principal Dr. Srinivas Reddy Sir of Aditya Engineering College, and to the management for providing a great support for our project completion.

**Y. Kranthi (16A95a0436)**

**N. Sudha (15A91A04G1)**

**B. Amit (15A91A04C3)**

**G.Indrani (16A95A0429)**

DECLARATION

We hereby declare that this project entitled “AWS CLOUD & NETWORK SECURITY” has been undertaken by us and this work has been submitted to ADITYA COLLEGE OF ENGINEERING affiliated to J.N.T.U Kakinada, in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Computer Science & Engineering.

We declare that our project entitled “AWS CLOUD & NETWORK SECURITY” is not submitted in any university.

**Project Associates**

Y. Kranthi (16A95a0436)

N. Sudha (15A91A04G1)

B. Amit (15A91A04C3)

G.Indrani (16A95A0429)

**INDEX**

Page Numbers

1. INTRODUCTION 1

2. REQUIREMENT ANALYSIS 1-2

2.1 Hardware Requirements.

2.2 Software Requirements

2.3 Services & Platforms

3.SYSTEM ANALYSIS 2

3.1 EXISTING SYSTEM

3.2 PROPOSED SYSTEM

4. SYSTEM DESIGN 2-5

4.1 UML Diagrams

4.1.1 Use Case Diagram

4.1.2 Activity Diagram

4.1.3 Sequence Diagram

5. AWS CLOUD 5-8

5.1 What is AWS and why AWS

6. Website and DB details 9-54

6.1 Main website code 9-28

6.2 IOT web page code 29-31

6.2.1 IoT Introduction 32-37

6.2.2 IoT Ardunio Code 38-43

6.2.3 MQTT Setup 44-46

6.3 Database Creation 46-47

6.3.1 Setting Database Path 47-48

6.3.2 Downloading and Installing Node js 48

6.3.3 Connecting Database to Website 48-49

6.4 Python MQTT Code 50-53

6.5 Storing Atmosphere details into Database tables 53-54

7. Amazon EC2 54-57

7.1 Procedure for running web scripts on server: 57-58

8. Elastic Load Balancer 58-64

9. AUTO SCALING 64-72

10. Network Security 72-85

10.1 DHCP Snooping 72-73

10.2 Implementing Port-Security 73-75

10.3 Securing the Cisco IOS Image and Configuration Files 75

10.4 ARP Dynamic Inspection 76

10.5 Site to Site VPN 77-85

11. Conclusion