

A Project Report on

AWS Cloud and Network Security

Submitted in partial fulfillment of the requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

ELECTRONICS & COMMUNICATION ENGINEERING

By

Yeluri Kranthi Babu	16A95A0436
Nersu Sudha Sai Sri	15A91A04G1
Gorrela Indrani	16A95A0429
Amit Raj Dev	15A91A04C3

Under the Esteemed guidance of

P. BALA SRINIVAS, M.Tech
Assistant Professor



**DEPARTMENT OF ELECTRONICS AND COMMUNICATION
ENGINEERING**

ADITYA ENGINEERING COLLEGE

An Autonomous Institution

(Approved by AICTE, New Delhi & Affiliated to JNTU, Kakinada)

ADITYA NAGAR, ADB ROAD, SURAMPALEM

2015-2019

ADITYA ENGINEERING COLLEGE

An Autonomous Institution

(Approved by AICTE, New Delhi & Affiliated to JNTU, Kakinada)

ADITYA NAGAR, ADB ROAD, SURAMPALEM

DEPARTMENT OF ELECTRONICS AND COMMUNICATION
ENGINEERING



CERTIFICATE

This is to certify that the project report entitled **“AWS Cloud And Network Security”** is a bonafide record of the project work done by

Yeluri Kranthi Babu	16A95A0436
Nersu Sudha Sai Sri	15A91A04G1
Gorrela Indrani	16A95A0429
Amit Raj Dev	15A91A04C3

under my supervision and guidance, for the partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in the Department of Electronics & Communication Engineering of Aditya Engineering College (A) from Jawaharlal Nehru Technological University, Kakinada for the year 2015-19.

Project Guide

Head of the Department

P.BALASRINIVAS

V.SATYANARAYANA

External Examiner

ACKNOWLEDGEMENT

We take this opportunity as a privilege to thank all individuals without whose support and guidance we could not have completed our project in this stipulated period of time.

We express our deep sense of gratitude to our guide **Mr. P. Bala Srinivas** for his valued suggestions and inputs during the course of the project work, readiness for consultation at all times, his educative comments and inputs, his concern and assistance even with practical things have been extremely helpful.

We highly indebted to our Head of the Department **Mr. V. Satyanarayana** for his motivational guidance and the vision in providing the necessary resources and timely inputs.

We are also thankful to **Dr. M. Sreenivasa Reddy**, Principal, Aditya Engineering College for providing appropriate environment required for this project and thankful to Faculty of Electronics and Communication Engineering Department for the encouragement and cooperation for this successful completion of the project.

Yeluri Kranthi Babu	16A95A0436
Nersu Sudha Sai Sri	15A91A04G1
Gorrela Indrani	16A95A0429
Amit Raj Dev	15A91A04C3

ABSTRACT

AWS Cloud is used 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.

This 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. Monitoring the atmosphere information of the area, In that temperature, humidity, raining status of the details. These are achieved by IoT Technology. 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. To connect different branches with security, we are implementing SITE TO SITE VPN. To overcome the network attacks, these network security infrastructure are implementing in On-premises, not in a cloud.

CONTENTS

	Page No
List of Figures	i
List of Tables	iii
Nomenclature	iv
1. INTRODUCTION	01-05
1.1 Requirements	01
1.2 Hardware Requirements	02
1.3 Software Requirements	02
1.4 Services and Platforms	02
1.5 Existing System	02
1.6 Proposed System	02
1.7 Use Case	03
1.8 Activity Diagram	04
1.9 Sequence Diagram	05
2. LITERATURE SURVEY	06-08
2.1 Introduction	06
2.1.1 Life Before Cloud Computing	06
2.2 Why Cloud Computing ?	07
2.3 Research Papers	07
3. AWS CLOUD	09-13
3.1 Why AWS?	09
3.2 What is Cloud Computing?	09
3.3 Cloud Computing Types	10
3.3.1 Infrastructure as a Service (IAAS)	10
3.3.2 Platform as a Service (PAAS)	12
3.3.3 Software as a Service (SAAS)	12
3.4 Advantages and Benefits of Cloud Computing	13
4. INTERNET OF THINGS	15-37
4.1 DHT11-Humidity and Temperature Sensor	15
4.2 Specifications	16
4.3 DHT11 Temperature and Humidity Sensor	19
4.4 Node MCU	20

4.4.1 DHT11 Sensor Connection with NodeMCU	31
4.5 Raindrop Sensor	21
4.6 Installation of Libraries	25
4.7 MQTT Protocol	25
4.7.1 Sending Sensor Data to Client through MQTT Protocol	27
4.7.2 Configure MQTT	28
5. AWS SERVICES	31-47
5.1 Introduction	31
5.1.1 Features of Amazon EC2	31
5.1.2 How to launch an EC2 instance on AWS	32
5.1.3 Execute the Following Commands on Gitbash Console	34
5.1.4 Procedure for Running Scripts on Server	35
5.1.5 Installing the Node Source Node.js 10	36
5.2 Elastic Load Balancer	36
5.2.1 Introduction	36
5.2.2 Advantages	37
5.2.3 How to add Load Balancer in AWS	37
5.3 AUTO SCALING	42
5.3.1 Introduction	42
5.3.2 Create a Launch Template	42
5.3.3 Create Auto-Scaling groups	45
6. NETWORK SECURITY	48-59
6.1 Introduction	48
6.2 DHCP Snooping	49
6.3 Port Security	50
6.4 Secured IOS and Configuration File	52
6.5 ARP Dynamic Inspection	53
6.4 Site to Site VPN	55
7. RESULTS	59-65
8. CONCLUSION AND FUTURE SCOPE	66
8.1 Conclusion	66
8.2 Future Scope	66
REFERENCES	67
APPENDIX	

LIST OF FIGURES

Figure No	Name of Figure	Page No
1.1	Scale In and Out Instances	04
1.2	AWS working	05
4.1	3-D View of DHT11 Sensor	19
4.2	DHT11 Sensor	20
4.3	Node MCU	20
4.4	Pin Diagram of Node MCU	21
4.5	Rain Drop Sensor	22
4.6	Schematic Diagram	23
4.7	Connecting of Rain Sensor with Node MCU	23
4.8	Rain Drop Sensor	24
4.9	Vaisala YL-83 Rain Detector	25
4.10	MQTT Protocol	26
4.11	MQTT Broker	27
4.12	MQTT Schematic Data Flow	27
4.13	MQTT Display INFO	28
5.1	Git Bash Console	34
5.2	Load Balancers	38
6.1	Network Topology	48
6.2	DHCP Snooping Output	50

6.3	Port Security Output	52
6.4	Secured IOS Output	53
6.5	Site to Site VPN	55
7.1	Main Website Page	60
7.2	EC2 Output	61
7.3	IOT Web Page	61
7.4	Load Balancer URL of website	62
7.5	Auto Scale in Output	62
7.6	Auto Scale Output	63
7.7	Auto Scale Final Output	64
7.8	DHCP Snooping Output	64
7.9	Port Security Output	65
7.10	Secured IOS Output	65
7.11	VPN Output	65

LIST OF TABLES

Table No	Name of Table	Page No
4.1	Ranges of DHT11 Sensor	16

NOMENCLATURE

SAAS	-	Software as a Service
IAAS	-	Infrastructure as a Service
PAAS	-	Platform as a Service
AWS	-	Amazon Web Services
ARP	-	Address Resolution Protocol
DHCP	-	Dynamic Host Configuration Protocol
MQTT	-	Message Queuing Telemetry Transport
URL	-	Uniform Resource Locator
EC2	-	Elastic Cloud Compute
LB	-	Load Balancer
AS	-	Auto Scale
IOS	-	Internetwork Operating System
VPN	-	Virtual Private Network
DB	-	Database