*A Project Report on*

**AWS Cloud and Network Security**

*Submitted in partial fulfilment of the requirements for the award of the degree of*

**BACHELOR OF TECHNOLOGY**

**IN**

**ELECTRONICS & COMMUNICATION ENGINEERING**

*By*

**Y. Kranthi 16A95A0436**

**N. Sudha 15A91A04G1**

**Amit Raj Dev 15A91A04C3**

**G. Indrani 16A95A0429**

*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

**Y. Kranthi 16A95A0436**

**N. Sudha 15A91A04G1**

**Amit Raj Dev 15A91A04C3**

**G. Indrani 16A95A0429**

under my supervision and guidance, for the partial fulfilment 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 2015-2019.

**Head of the Department**

**V.SATYANARAYANA**

**Project Guide**

**P. BALA SRINIVAS**

**External Examiner**

**ACKNOWLEDGMENT**

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 ot 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.

**Y. Kranthi 16A95A0436**

**N. Sudha 15A91A04G1**

**Amit Raj Dev 15A91A04C3**

**G. Indrani 16A95A0429**

**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 infrastructures are implementing in On-premises, not in a cloud.