Software Requirement Specifications

1.1 Purpose

The aim of this SRS document is to explain the functionality of Network Traffic Analyzer for detecting Dos attack using ML.

It is the outcome based on the requirements of the customer, by the various groups.

This document will provide a baseline for designing, coding & evaluation of test plans. It will be used as a solid foundation for continued product evaluation.

Our system helps in detecting the Dos Attacks before entering the internal network.

1.2 Definitions, Acronyms, and abbreviations Acronyms

C-DAC	Center for Development of Advanced Computing
SRS	Software Requirement Specifications
ML	Machine Learning

1.3 References for Requirement Analysis and Design

- Catalogues
- IEEE Recommended Practices for SRS. ANSI / IEEE Std 830 – 1993.
- Different documents, registers related to Network traffic analyzer for detecting Dos attacks using Machine Learning.

1.4 Overview

The remaining part of SRS consists of

- Complete description of the various product functions.
- Logical characteristics of product functions.
- Hardware and software configuration for servers and clients operating at various levels.

Business Model:

- “Network Traffic Analyzer For Detecting Dos Attack Using Machine Learning” analysis the incoming packets and determines whether it is normal traffic or some malicious packets in particular denial of service attack.
- Using machine learning the system is trained to classify the incoming traffic as normal traffic or Dos attack.
- The tools used to achieve this are Tshark, anaconda navigator, matplotlib and scikit learn.
- Using Tshark the incoming packets are captured and sent as a CSV file to Pandas which perform data analysis to differentiate normal packets and Dos packets and then we visualize (Bar graphs) the normal and Dos packets by using Matplotlib later, we implement ML to train the System so that it will detect and classifies the Dos packets.

Table of Contents

- **List of Functions**

Sr. No.	**Function ID**	**Name of Function**
•	F-1	Generating the network traffic.
•	F-2	Capturing the traffic.
•	F-3	Analyzing and detecting the Dos attack.
•	F-4	Visualize the attack and stop the attack.

2. Functional Description :

F-1. Function : **Generating the network traffic.**

Function ID : F-1

Purpose : We will generate traffic through different machines and all the traffic goes through the network traffic analysis software i.e. inside our server.

Task Performed by : Anshul, Chandan,Sumesh and Bhargavi

Time (When Performed) : First two weeks

F-2. Function **Capturing the Traffic.**

Function ID : F-2

Purpose **:** Here we use Tshark .TShark is a network protocol analyzer which capture packet data from a live network, or read packets from a previously saved capture file, either printing a decoded form of those packets to the standard output or writing the packets to a file.

Task Performed by : All Team members.

Time (When Performed : After 2 weeks

F-3. Function **Analyzing and detecting the Dos attack.**

Function ID **:** F-3

Purpose **:** By using Pandas/NumPy and Scikit Learn we Analyze and detect the Dos Attack. Pandas is a Python package providing fast, flexible, and expressive data structures designed to make working with “relational” or “labeled” data both easy and intuitive. It aims to be the fundamental high-level building block for doing practical, real world data analysis in Python.And we use Scikit Learn to train the System with Dos packets.

Performed By **:** All Team members

Time (When Performed) **:** After 3 weeks

F-4. Function **Visualize and stop the attack**

Function ID **:** F-5

Purpose **:** Now we will visualize the attack by using Matplotlib. Matplotlib is a plotting library for the Python programming language and its numerical mathematics extension NumPy. It provides an object-oriented API for embedding plots into applications using general-purpose GUI toolkits like Tkinter, wxPython, Qt, or GTK+.

Performed By **:** All Team members

Time (When Performed) **:** After 7 weeks

3. Hardware & Network Interfaces

➪ Back-end Server Configuration

- Intel Pentium-IV
- 128 MB RAM
- 1 Raid Controller Card
- 32 bit Ethernet Controller (100 Base T)
- 8 x 2.0 GB Fast SCSI/2 with Raid Support
- 2.88 MB FDD
- 48 x CD ROM Drive

➪ Front-end Client Configuration

- Intel Pentium-III @ 650 MHz
- 128 MB SDRAM
- 10 GB Hard Disk Drive
- 1.44 MB Floppy Disk Drive
- 15" SVGA Digital Color Monitor

- One Serial, One Parallel pond One USB port.
- 104 Keys Keyboard
- PS2 Mouse with pad
- 32 bit PCI Ethernet Card
- 48X CD Drive

- **Software Interfaces**

➪ Software configuration for back-end Services

- Windows 10
- Linux
- Wiresshark /Tshark
- Panadas /Numpy
- Scikit-learn

➪ Software configuration for front-end Services

- Matplotlib

- **Communication Interfaces**

Various network protocols such as ISDN, ATM will be used for Intranet connectivity. UTP Ethernet, TCP/IP Protocols will be used for Local Area Networks. Network hubs, routers, bridges, cables, patch cables, connectors will be required.