Functional Document for DDoS Detection Research Project

1. Introduction

The DDoS Detection Research Project aims to enhance network security by developing advanced detection models using traditional machine learning, deep learning, and hybrid quantum techniques. This document outlines the key goals and features of the project, focusing on implementing and comparing K-Nearest Neighbors (KNN), Convolutional Neural Networks (CNN), and Hybrid Quantum Neural Networks (H-QNN) for effective DDoS attack detection.

2. Product Goal

The primary goal of this research project is to develop and evaluate robust models for detecting DDoS attacks, improving detection accuracy, and minimizing false positives. This contributes to the overarching objective of advancing cybersecurity measures in a world increasingly reliant on digital infrastructure.

3. Demography (Users, Location)

Users

- **Target Users**: Network administrators, cybersecurity analysts, and IT security teams.
- **User Characteristics:** Varying levels of technical expertise, with a focus on professionals in cybersecurity and IT management.

Location

- **Target Location**: Global usage, with a particular focus on organizations vulnerable to cyber threats, such as businesses, government agencies, and educational institutions.

4. Business Processes

The key business processes include:

Data Preparation:

- Process for collecting and preprocessing network traffic data for model training.

Model Development:

- Process for developing KNN, CNN, and H-QNN models, including training, validation, and testing phases.

Model Evaluation:

- Process for evaluating model performance based on metrics such as accuracy, precision, recall, and F1-score.

5. Features

This project will focus on implementing the following key features:

KNN Model Implementation:

Develop a baseline DDoS detection model using KNN, with emphasis on hyperparameter tuning and feature selection.

CNN Model Development:

Create a deep learning model to capture complex patterns in network traffic data, improving detection rates for sophisticated DDoS attacks.

Hybrid Quantum Neural Network (H-QNN):

Integrate quantum computing techniques with classical neural networks to enhance feature extraction and classification efficiency.

6. Authorization Matrix

Define the roles and their corresponding access levels:

Role	Access Level
Data Scientist	Full access to data preprocessing and model development tools.
Cybersecurity Analyst	Access to model evaluation and reporting functionalities.
Project Manager	Access to all project documentation and progress reports.
Research Collaborator	Access to specific datasets and models for research purposes.

7. Assumptions

- The development environment and infrastructure (including computational resources) will remain stable throughout the project.
- Stakeholders, including cybersecurity experts and data scientists, will be available for feedback and clarification during the development process.
- Team members possess the necessary skills and resources to implement and validate machine learning and quantum models effectively.