Software Requirements Specification (SRS) for SpamGuard

Software Requirements Specification (SRS) for SpamGuard

Table of Contents

1. Introduction

1.1 Purpose

The purpose of this document is to provide a detailed specification of the requirements for the SpamGuard application. It is intended for developers, testers, and stakeholders to understand the functionalities and constraints of the system.

1.2 Scope

SpamGuard is a web-based application designed to classify email content as spam or not spam using advanced AI algorithms. The application provides real-time analysis and a user-friendly interface for users to interact with the system.

1.3 Definitions, Acronyms, and Abbreviations

- **AI**: Artificial Intelligence
- **API**: Application Programming Interface
- **UI**: User Interface
- **JSON**: JavaScript Object Notation

1.4 References

- Node.js Documentation
- Express.js Documentation

- Google Generative AI API Documentation

2. Overall Description

2.1 Product Perspective

SpamGuard is an independent web application that leverages Google's Generative AI for email content analysis. It consists of a backend server and a frontend interface.

2.2 Product Functions

- Classify email content as spam or not spam.
- Provide a confidence score and reasons for classification.
- Offer a user-friendly interface for input and result display.

2.3 User Classes and Characteristics

- **End Users**: Individuals who want to check if an email is spam.
- **Administrators**: Manage the application and monitor its performance.

2.4 Operating Environment

- **Backend**: Node.js environment
- **Frontend**: Modern web browsers (Chrome, Firefox, Safari, Edge)

2.5 Design and Implementation Constraints

- Must use Google Generative AI for content analysis.
- Environment variables must be managed securely.

2.6 User Documentation

- User guide for navigating the application.
- FAQ section for common issues.

2.7 Assumptions and Dependencies

- Users have access to the internet.
- The Google Generative AI API is available and operational.

3. Specific Requirements

3.1 Functional Requirements

- **FR1**: The system shall accept email content input from the user.

- **FR2**: The system shall classify the email content using AI.
- **FR3**: The system shall return a JSON response with classification details.
- **FR4**: The system shall display the results to the user in a readable format.

4. External Interface Requirements

4.1 User Interfaces

- A web-based interface for inputting email content and displaying results.

4.2 Hardware Interfaces

- No specific hardware interfaces required.

4.3 Software Interfaces

- Integration with Google Generative AI API.

4.4 Communications Interfaces

- HTTP/HTTPS for client-server communication.

5. System Features

5.1 Real-time Spam Detection

- Users can input email content and receive immediate feedback.

5.2 Detailed Analysis

- Provides a confidence score, reasons for classification, and a risk level.

6. Non-functional Requirements

6.1 Performance Requirements

- The system should process and return results within 5 seconds.

6.2 Security Requirements

- Secure handling of API keys and user data.

6.3 Usability Requirements

- The interface should be intuitive and easy to navigate.

6.4 Reliability Requirements

- The system should have an uptime of 99.9%.

7. Other Requirements

7.1 Legal and Regulatory Requirements

- Compliance with data protection regulations (e.g., GDPR).

7.2 Environmental Requirements

- None specified.