**COMSATS University Islamabad,**

**Abbottabad Campus**

**SOFTWARE REQUIREMENTS SPECIFICATION   
(SRS DOCUMENT)**

**for**

**SMS SPAM FILTERING**  
Version 1.0

***By***

**Waseem Ullah CIIT/FA20-BSE-129/ATD**

**Muhammad Adeel CIIT/ FA20-BSE-163/ATD**

**Sooraj Lal CIIT/ FA20-BSE-004/ATD**

***Supervisor*Supervisor Name: Muhammad Ali Faisal**

***Bachelor of Science in Computer Science (2020-2024)***

**Table of Contents**

**Revision History 3**

**1.** **Introduction 5**

1.1 Purpose 5

1.2 Scope 5

**2.** **Overall description 6**

2.1 Product perspective 6

2.2 Operating environment 6

2.3 Design and implementation constraints 6

**3.** **Requirement identifying technique 7**

3.1 Use Case Diagram 7

3.2 Use Case Description 8

**4.** **Functional Requirement 17**

**5. Non-Functional Requirement 23**

**6. Project Gantt Chart 29**

**7.** **References 29**

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Date** | **Reason for changes** | **Version** |
|  |  |  |  |
|  |  |  |  |

**Application Evaluation History**

|  |  |
| --- | --- |
| **Comments (by committee)**  **\*include the ones given at scope time both in doc and presentation** | **Action Taken** |
|  |  |
|  |  |

**Supervised by**

**<Supervisor’s Name>**

Signature\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Introduction:**

This document outlines the **Software Requirements Specification (SRS)** for the SMS Spam Filtering System. It aims to provide a detailed description of the requirements, features, and functionalities of the system. The document is organized to facilitate understanding and utilization by project stakeholders, including developers, testers, and project managers.

**Purpose:**

The purpose of this document is to clearly define the requirements for the development of the SMS Spam Filtering System. It serves as a comprehensive guide for all project stakeholders, ensuring a common understanding of the system's goals, functionalities, and constraints. Developers will use this document as a reference to implement the system, while testers will refer to it for validation and verification purposes.

**Scope:**

The SMS Spam Filtering System is designed to address the increasing issue of SMS spam, providing a robust solution to filter unwanted messages and enhance user privacy and security. The scope of the project includes the following key aspects:

* **Message Categorization:** The system categorizes incoming SMS messages into spam and non-spam categories based on content analysis, sender reputation, and user-defined preferences.
* **Real-Time Detection:** Utilizing real-time detection techniques, the system swiftly identifies and filters out spam messages before reaching the user's inbox.
* **Customization and User Interaction:** The system offers a user-friendly interface for customization of spam filtering settings. Users can review filtered messages, report false positives/negatives, and provide feedback for system improvement.
* **Scalability and Efficiency:** Engineered for scalability, the system efficiently handles increasing SMS message volumes while maintaining a seamless user experience.
* **Continuous Improvement:** Regular updates and model retraining ensure the system adapts to emerging spam threats, maintaining effectiveness over time.
* **Privacy and Regulatory Compliance:** The system prioritizes user privacy, processing data locally or in a secure environment, adhering to relevant privacy and data protection regulations.
* **Exclusion of Other Communication Types:** The focus remains on SMS-based spam filtering, excluding other forms of communication such as email or phone calls.

**Overall description**

**Product Perspective:**

The SMS Spam Filtering System is a standalone application designed to operate as an independent solution for mitigating the issue of SMS spam. It is not a replacement for an existing application but rather a novel system developed to enhance user privacy and security in the realm of SMS communication.

**Operating Environment**

**OE-1: Hardware Platform**

* + The system shall operate on standard mobile devices running Android operating systems, including smartphones and tablets.

**OE-2: Operating Systems**

* + The system shall be compatible with Android versions 8 and above.

**OE-3: Geographical Locations**

* + The system is intended for global use and shall operate seamlessly across various geographical locations.

**OE-4: Server and Database Hosting**

* + The system's servers and databases shall be hosted in a secure and compliant data center, ensuring data privacy and protection.

**Design and Implementation Constraints:**

**CO-1: Programming Language**

* + The system shall be implemented using the React Native framework for cross-platform mobile application development.

**CO-2: Database Engine**

* + The system shall utilize Firebase Fire store as the database engine to store user preferences, filter settings, and other relevant data.

**CO-3: SMS Processing**

* + The system shall rely on standard SMS APIs provided by mobile operating systems for message interception, categorization, and real-time processing.

**CO-4: User Interface Design Tools**

* + The system's user interface shall be designed using React Native for consistency across Android platforms.

**CO-5: Agile Methodology**

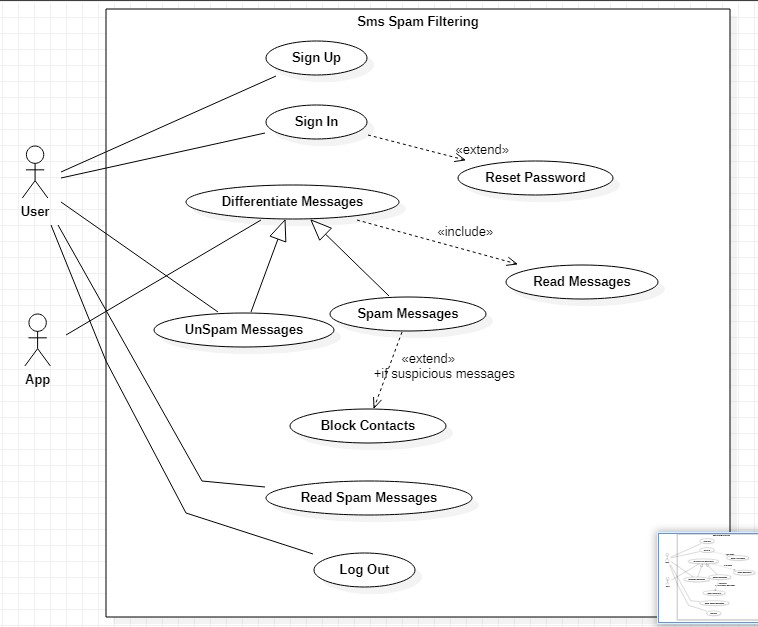
* + The development process shall adhere to the Agile methodology, emphasizing iterative and incremental development, client collaboration, and adaptability to changing requirements.

**Requirement identifying technique:**

**Brainstorming:** We have sat in a team and ask all the members to give their opinion on this system.

**Observation:** We observed by our own experience and our seniors that this type of application should be deployed to filter the spam and non-spam messages

**Use case Diagram:**



**Use case description:**

**Table 1 detail use case 1**

|  |  |
| --- | --- |
| **Use Case ID:** | UC-1 |
| **Use Case Name:** | Sign Up |
| **Actors:** | Primary Actor: User  Secondary Actors: None |
| **Description:** | A User creates a new user account in the SMS Spam Filtering System. |
| **Trigger:** | A User visits the SMS Spam Filtering System and clicks on the "Sign Up" button. |
| **Preconditions:** | None |
| **Postconditions:** | The User has a new user account in the SMS Spam Filtering System. |
| **Normal Flow:** | 1. The User enters their name, email address, and password into the sign-up form. 2. The User clicks on the "Sign Up" button. 3. The system validates the Users input and creates a new user account. 4. The system sends the User a confirmation email. 5. The User clicks on the confirmation link in the email to activate their account. 6. The User is logged into the SMS Spam Filtering System. |
| **Alternative Flows:** | **Sign Up Failed:** If the Users input is invalid, the system displays an error message and the User must re-enter their information.  **Account Already Exists:** If the Users email address is already associated with an existing account, the system displays a message and prompts the User to log in or reset their password. |
| **Exceptions:** | System Unavailable: If the SMS Spam Filtering System is unavailable, the User will not be able to sign up. |
| **Business Rules** | The User's email address must be unique.  The User's password must be at least 8 characters long and contain a mix of upper and lowercase letters, numbers, and symbols. |
| **Assumptions:** | 1. The User has access to an email account. 2. The User can connect to the Internet. |

**Table 2 detail use case 2**

|  |  |
| --- | --- |
| **Use Case ID:** | UC-2 |
| **Use Case Name:** | Sign in |
| **Actors:** | Primary Actor: User  Secondary Actors: None |
| **Description:** | A User who has already created an account in the SMS Spam Filtering System logs in to their account. |
| **Trigger:** | The User visits the SMS Spam Filtering System and clicks on the "Sign In" button. |
| **Preconditions:** | The User has a valid user account in the SMS Spam Filtering System. |
| **Postconditions:** | The User is logged into the SMS Spam Filtering System. |
| **Normal Flow:** | 1. The User enters their email address and password into the sign-in form. 2. The User clicks on the "Sign In" button. 3. The system validates the User's credentials. 4. If the credentials are valid, the User is logged into the system. 5. If the credentials are invalid, the system displays an error message and prompts the User to try again. |
| **Alternative Flows:** | **Password Reset:** If the User has forgotten their password, they can click on the "Forgot Password" link and follow the instructions to reset their password. |
| **Exceptions:** | System Unavailable: If the SMS Spam Filtering System is unavailable, the User will not be able to sign in. |
| **Business Rules** | The User's email address and password must match the credentials stored in the system.  If the User enters an incorrect password multiple times, their account will be locked. |
| **Assumptions:** | 1. The User has access to an email account. 2. The User can connect to the Internet. |

**Table 3 detail use case 3**

|  |  |
| --- | --- |
| **Use Case ID:** | UC-3 |
| **Use Case Name:** | Reset Password |
| **Actors:** | Primary Actor: User  Secondary Actors: None |
| **Description:** | A User who has forgotten their password resets it and regains access to their account in the SMS Spam Filtering System. |
| **Trigger:** | The User clicks on the "Forgot Password" link on the sign-in page. |
| **Preconditions:** | The User has a valid user account in the SMS Spam Filtering System.  The User has access to the email address associated with their account. |
| **Postconditions:** | The User's password has been reset.  The User can log in to their account using the new password. |
| **Normal Flow:** | 1. The User enters their email address into the "Forgot Password" form. 2. The User clicks on the "Reset Password" button. 3. The system sends a password reset email to the User's email address. 4. The User clicks on the password reset link in the email. 5. The User enters a new password and confirms it. 6. The system validates the User's new password and updates their account information. 7. The User is logged into their account using the new password. |
| **Alternative Flows:** | **Invalid Email Address:** If the User enters an invalid email address, the system displays an error message and prompts the User to try again.  **Email Not Sent:** If the system fails to send the password reset email, the User is notified and can request assistance from support. |
| **Exceptions:** | System Unavailable: If the SMS Spam Filtering System is unavailable, the User will not be able to reset their password. |
| **Business Rules** | The User's new password must be at least 8 characters long and contain a mix of upper and lowercase letters, numbers, and symbols.  The User must confirm their new password correctly. |
| **Assumptions:** | 1. The User has access to an email account. 2. The User can connect to the Internet. |

**Table 4 detail use case 4**

|  |  |
| --- | --- |
| **Use Case ID:** | UC-4 |
| **Use Case Name:** | Differentiate Messages |
| **Actors:** | Primary Actor: User  Secondary Actors: None |
| **Description:** | A User who has forgotten their password resets it and regains access to their account in the SMS Spam Filtering System. |
| **Trigger:** | The User clicks on the "Forgot Password" link on the sign-in page. |
| **Preconditions:** | The User has a valid user account in the SMS Spam Filtering System.  The User has access to the email address associated with their account. |
| **Postconditions:** | The User's password has been reset.  The User can log in to their account using the new password. |
| **Normal Flow:** | 1. The User enters their email address into the "Forgot Password" form. 2. The User clicks on the "Reset Password" button. 3. The system sends a password reset email to the User's email address. 4. The User clicks on the password reset link in the email. 5. The User enters a new password and confirms it. 6. The system validates the User's new password and updates their account information. 7. The User is logged into their account using the new password. |
| **Alternative Flows:** | **Invalid Email Address:** If the User enters an invalid email address, the system displays an error message and prompts the User to try again.  **Email Not Sent:** If the system fails to send the password reset email, the User is notified and can request assistance from support. |
| **Exceptions:** | System Unavailable: If the SMS Spam Filtering System is unavailable, the User will not be able to reset their password. |
| **Business Rules** | * The User's new password must be at least 8 characters long and contain a mix of upper and lowercase letters, numbers, and symbols. * The User must confirm their new password correctly. |
| **Assumptions:** | 1. The User has access to an email account. 2. The User can connect to the Internet. |

**Table 5 detail use case 5**

|  |  |
| --- | --- |
| **Use Case ID:** | UC-5 |
| **Use Case Name:** | Unspamming Messages |
| **Actors:** | Primary Actor: User  Secondary Actors: SMS Spam Filtering SystemSecondary Actors: None |
| **Description:** | A User utilizes the SMS Spam Filtering System to identify and filter out unwanted or unsolicited messages, commonly known as spam. This helps to protect the User from disruptive, annoying, and potentially fraudulent messages. |
| **Trigger:** | The User receives an SMS message and suspects that it may be spam. |
| **Preconditions:** | The User is logged into the SMS Spam Filtering System.  The User has received an SMS message. |
| **Postconditions:** | The User has identified the received SMS message as spam or not spam.  The User has the option to filter out or block spam messages. |
| **Normal Flow:** | 1. The User receives an SMS message. 2. The User analyzes the content of the SMS message for indications of spam, such as suspicious links, promotional offers, or deceptive language. 3. The User consults the SMS Spam Filtering System's spam filtering tools to further evaluate the message. 4. The SMS Spam Filtering System analyzes the message using content-based filtering, sender reputation filtering, real-time blacklists, or machine learning algorithms. 5. The SMS Spam Filtering System provides the User with a classification of the message as spam or not spam. 6. The User can choose to filter out the spam message, preventing it from appearing in their inbox, or block the sender to prevent future messages from being received. |
| **Alternative Flows:** | **Unsure Message:** If the User is unsure whether the message is spam or not spam, they can tag the message for further review or seek assistance from support.  **False Positive:** If a legitimate message is incorrectly classified as spam, the User can notify the system to improve its accuracy. |
| **Exceptions:** | System Unavailable: If the SMS Spam Filtering System is unavailable, the User may not be able to accurately classify or filter spam messages. |
| **Business Rules** | * The SMS Spam Filtering System should continuously learn and adapt to identify new spam tactics and minimize false positives. * The User should have control over their spam filtering settings, allowing them to adjust sensitivity levels or whitelist specific senders. * The SMS Spam Filtering System should provide clear and easy-to-use tools for identifying, filtering, and blocking spam messages. |
| **Assumptions:** | 1. The User has access to the SMS Spam Filtering System. 2. The User understands the characteristics of spam messages. 3. The User has a reliable internet connection. |

**Table 6 detail use case 6**

|  |  |
| --- | --- |
| **Use Case ID:** | UC-6 |
| **Use Case Name:** | Spam Messages |
| **Actors:** | Primary Actor: User  Secondary Actors: SMS Spam Filtering System |
| **Description:** | A User utilizes the SMS Spam Filtering System to identify, filter, and block spam messages. The User can also report spam messages to improve the system's accuracy and protect other users. |
| **Trigger:** | The User receives an SMS message. |
| **Preconditions:** | The User is logged into the SMS Spam Filtering System.  The User has received an SMS message. |
| **Postconditions:** | The User has identified the received SMS message as spam or not spam.  The User has filtered or blocked the spam message (if applicable).  The User has reported the spam message (if applicable). |
| **Normal Flow:** | 1. The User receives an SMS message. 2. The SMS Spam Filtering System analyzes the message using content-based filtering, sender reputation filtering, real-time blacklists, or machine learning algorithms. 3. The SMS Spam Filtering System classifies the message as spam or not spam. 4. The User is notified of the message classification and given options to: 5. View the message content (if not already visible) 6. Mark the message as spam or not spam (if the system's classification is incorrect) 7. Filter the message to a dedicated spam folder 8. Block the sender to prevent future messages from being received 9. Report the message to the SMS Spam Filtering System for further analysis and improvement |
| **Alternative Flows:** | **Unsure Message:** If the User is unsure whether the message is spam or not spam, they can tag the message for further review or seek assistance from support.  **False Positive:** If a legitimate message is incorrectly classified as spam, the User can notify the system to improve its accuracy.  **Reported Message:** When a User reports a spam message, the SMS Spam Filtering System analyzes the message and updates its filtering algorithms to better identify similar spam messages in the future. |
| **Exceptions:** | System Unavailable: If the SMS Spam Filtering System is unavailable, the User may not be able to accurately classify or filter spam messages. |
| **Business Rules** | * The SMS Spam Filtering System should continuously learn and adapt to identify new spam tactics and minimize false positives. * The User should have control over their spam filtering settings, allowing them to adjust sensitivity levels or whitelist specific senders. * The SMS Spam Filtering System should provide clear and easy-to-use tools for identifying, filtering, and blocking spam messages. |
| **Assumptions:** | 1. The User has access to the SMS Spam Filtering System. 2. The User understands the characteristics of spam messages. 3. The User has a reliable internet connection. |

**Table 7 detail use case 7**

|  |  |
| --- | --- |
| **Use Case ID:** | UC-7 |
| **Use Case Name:** | Read Messages |
| **Actors:** | Primary Actor: User  Secondary Actors: None |
| **Description:** | A User accesses and views their messages within the SMS Spam Filtering System. This includes messages in their inbox, sent messages, and archived messages. |
| **Trigger:** | The User logs into the SMS Spam Filtering System and navigates to their message inbox. |
| **Preconditions:** | The User is logged into the SMS Spam Filtering System.  The User has access to their SMS messages. |
| **Postconditions:** | The User has reviewed and viewed their messages.  The User has identified specific messages for further action, such as replying, forwarding, or deleting. |
| **Normal Flow:** | 1. The User logs into the SMS Spam Filtering System using their credentials. 2. The User selects the "Inbox" tab to view their received messages. 3. The system retrieves and displays the User's messages in chronological order, with the most recent message at the top. 4. The User can view the message content, sender information, timestamp, and attachments (if applicable). 5. The User can perform actions on individual messages, such as: 6. Replying to the message 7. Forwarding the message to another recipient 8. Deleting the message 9. Archiving the message for future reference 10. The User can utilize search filters to narrow down the displayed messages based on sender, date, keywords, or other criteria. 11. The User can navigate between different message folders, such as "Sent Items" or "Archived Items," to view their respective messages. |
| **Alternative Flows:** | **Empty Inbox:** If the User has no unread messages, the system displays a message indicating an empty inbox.  **Message Search:** If the User utilizes search filters, the system retrieves and displays messages matching the specified criteria.  **Message Navigation:** The User can access different message folders, such as "Sent Items" or "Archived Items," to view their respective messages. |
| **Exceptions:** | **System Unavailable:** If the SMS Spam Filtering System is unavailable, the User will not be able to access their messages. |
| **Business Rules** | * The SMS Spam Filtering System should provide a clear and organized message interface for easy navigation and message viewing. * The system should enable efficient search and filtering capabilities to allow Users to quickly locate specific messages. * Message sorting options should be available to organize messages based on various criteria, such as sender, date, or importance. |
| **Assumptions:** | 1. The User has a reliable internet connection. 2. The User is familiar with the SMS Spam Filtering System interface. 3. The User has an understanding of basic message management tasks. |

**Table 8 detail use case 8**

|  |  |
| --- | --- |
| **Use Case ID:** | UC-8 |
| **Use Case Name:** | Block Contacts |
| **Actors:** | Primary Actor: User  Secondary Actors: SMS Spam Filtering System |
| **Description:** | A User utilizes the SMS Spam Filtering System to block specific contacts, preventing them from sending further SMS messages to the User's phone number. |
| **Trigger:** | The User receives an unwanted or harassing SMS message from a contact they wish to block. |
| **Preconditions:** | The User is logged into the SMS Spam Filtering System.  The User has received an SMS message from the contact they want to block. |
| **Postconditions:** | The User has blocked the specified contact.  Future SMS messages from the blocked contact will not be received by the User. |
| **Normal Flow:** | 1. The User receives an unwanted or harassing SMS message from a contact they wish to block. 2. The User identifies the sender's phone number or contact information. 3. The User accesses the SMS Spam Filtering System's contact management settings. 4. The User selects the "Block Contacts" option. 5. The User enters or selects the phone number or contact information of the contact they want to block. 6. The User confirms their decision to block the contact. 7. The system adds the specified contact to the User's block list. 8. Future SMS messages from the blocked contact will be automatically filtered and not delivered to the User's phone number. |
| **Alternative Flows:** | **Contact Search:** The User can utilize the system's contact search feature to locate the contact they want to block.  **Multiple Contacts:** The User can block multiple contacts simultaneously by selecting or adding them to the block list.  **Contact Unblocking:** If the User wishes to unblock a contact, they can remove the contact from their block list. |
| **Exceptions:** | System Unavailable: If the SMS Spam Filtering System is unavailable, the User will not be able to access their block list or block contacts. |
| **Business Rules** | * The SMS Spam Filtering System should provide a clear and easy-to-access block list management feature. * The system should allow Users to block contacts based on phone numbers, contact names, or other identifying information. * The system should prevent blocked contacts from sending SMS messages to the User's phone number, even if the blocked contact changes their phone number. |
| **Assumptions:** | 1. The User has a reliable internet connection. 2. The User is familiar with the SMS Spam Filtering System interface. 3. The User understands the purpose and implications of blocking contacts. |

**Table 9 detail use case 9**

|  |  |
| --- | --- |
| **Use Case ID:** | UC-9 |
| **Use Case Name:** | Read Spam Messages |
| **Actors:** | Primary Actor: User  Secondary Actors: None |
| **Description:** | A User accesses and reviews their identified spam messages within the SMS Spam Filtering System. This allows them to review the messages, identify any potential false positives, and report genuine spam messages to further improve the system's accuracy. |
| **Trigger:** | The User navigates to the "Spam" folder or section within the SMS Spam Filtering System. |
| **Preconditions:** | The User is logged into the SMS Spam Filtering System.  The User has spam messages identified and categorized by the system's spam filtering algorithms. |
| **Postconditions:** | The User has reviewed and viewed their identified spam messages.  The User has identified any potential false positives and taken appropriate action, such as marking them as not spam.  The User has reported genuine spam messages to the system to improve its accuracy. |
| **Normal Flow:** | 1. The User logs into the SMS Spam Filtering System using their credentials. 2. The User selects the "Spam" folder or section to view their identified spam messages. 3. The system retrieves and displays the User's spam messages in chronological order, with the most recent message at the top. 4. The User can view the message content, sender information, timestamp, and attachments (if applicable). 5. The User can perform actions on individual spam messages, such as: 6. Marking the message as "Not Spam" if it was incorrectly classified 7. Replying to the message (if necessary) 8. Forwarding the message to another recipient (if relevant) 9. Deleting the message 10. Reporting the message as genuine spam to improve the system's accuracy 11. The User can utilize search filters to narrow down the displayed spam messages based on sender, date, keywords, or other criteria. 12. The User can navigate between different message folders, such as "Inbox" or "Archived Items," to view their respective messages. |
| **Alternative Flows:** | **Empty Spam Folder:** If the User has no spam messages, the system displays a message indicating an empty spam folder.  **Message Search:** If the User utilizes search filters, the system retrieves and displays spam messages matching the specified criteria.  **Message Navigation:** The User can access different message folders, such as "Inbox" or "Archived Items," to view their respective messages. |
| **Exceptions:** | **System Unavailable:** If the SMS Spam Filtering System is unavailable, the User will not be able to access their spam messages. |
| **Business Rules** | * The SMS Spam Filtering System should provide a clear and organized message interface for easy navigation and spam message viewing. * The system should enable efficient search and filtering capabilities to allow Users to quickly locate specific spam messages. * Message sorting options should be available to organize spam messages based on various criteria, such as sender, date, or importance. |
| **Assumptions:** | 1. The User has a reliable internet connection. 2. The User is familiar with the SMS Spam Filtering System interface. 3. The User has an understanding of basic message management tasks. |

**Table 10 detail use case 10**

|  |  |
| --- | --- |
| **Use Case ID:** | UC-10 |
| **Use Case Name:** | Log Out |
| **Actors:** | Primary Actor: User  Secondary Actors: None |
| **Description:** | A User securely terminates their current session within the SMS Spam Filtering System, effectively logging out and preventing unauthorized access to their account.. |
| **Trigger:** | The User initiates the logout process by selecting the designated logout option or button. |
| **Preconditions:** | The User is currently logged into the SMS Spam Filtering System.  The User has access to the logout option or button. |
| **Postconditions:** | The User has successfully logged out of the SMS Spam Filtering System.  The User's session has been terminated, preventing further access to their account without re-entering their credentials.  The User's privacy and security are protected from unauthorized access. |
| **Normal Flow:** | 1. The User clicks on the designated "Log Out" button or selects the logout option from the menu. 2. The system prompts the User for confirmation to ensure they intend to log out. 3. Upon confirmation, the system invalidates the User's current session token and terminates their active session. 4. The system redirects the User to the login page, indicating they are now logged out. |
| **Alternative Flows:** | **Inactive Session:** If the User's session has already expired due to inactivity, the system will automatically redirect them to the login page.  **Unexpected Logout:** If the User accidentally clicks the "Log Out" button, they can immediately navigate back to the login page and re-enter their credentials to regain access to their account. |
| **Exceptions:** | **System Unavailable:** If the SMS Spam Filtering System is unavailable, the User may not be able to initiate the logout process. |
| **Business Rules** | * The SMS Spam Filtering System should implement a secure logout mechanism that invalidates session tokens and terminates active sessions upon logout. * The system should provide a clear and accessible logout option to facilitate easy user logout. * The system should prevent unauthorized access to a User's account after they have logged out. |
| **Assumptions:** | 1. The User has a reliable internet connection. 2. The User understands the purpose and implications of logging out. |

**Functional Requirements:**

* **Feature: SMS Submission**

**FR-1:** The user shall be able to submit an SMS message to the system for spam filtering.

**FR-2:** The system shall accept SMS messages in a variety of formats, such as plain text, SMS-PDU, and WAP-PDU.

**FR-3:** The system shall store submitted SMS messages for processing and spam filtering.

* **Feature: SMS Spam Filtering**

**FR-4:** The system shall be able to identify and classify SMS messages as spam or non-spam.

**FR-5:** The system shall use a machine learning algorithm to classify SMS messages.

**FR-6:** The system shall achieve a spam filtering accuracy of at least 95%.

* **Feature: Spam Reporting**

**FR-7:** The user shall be able to report an SMS message as spam.

**FR-8:** The system shall store reported SMS messages for analysis and improvement of the spam filtering algorithm.

* **Feature: User Interface**

**FR-9:** The system shall have a user-friendly interface that allows users to easily submit SMS messages, view spam filtering results, and report spam.

**FR-10:** The system shall provide clear and concise information about the spam filtering process and results.

**FR-11:** The system shall be accessible to users with disabilities.

* **Feature: Performance**

**FR-12:** The system shall be able to filter SMS messages in real time.

**FR-13:** The system shall be able to handle the volume of SMS messages received.

* **Feature: Security**

**FR-14:** The system shall be secure and protect user data from unauthorized access.

**FR-15:** The system shall implement appropriate security measures, such as user authentication and data encryption..

* **Functional Requirement Tables:**

**Functional Requirement Table 1**

|  |  |
| --- | --- |
| **Identifier** | FR-1 |
| **Title** | SMS Submission |
| **Requirement** | The user shall be able to submit an SMS message to the system for spam filtering. |
| **Source** | User |
| **Rationale** | To enable the system to perform spam filtering |
| **Business Rule (if required)** | The user must provide the SMS message to be filtered. |
| **Dependencies** | None |
| **Priority** | High |

**Functional Requirement Table 2**

|  |  |
| --- | --- |
| **Identifier** | FR-2 |
| **Title** | SMS Spam Filtering |
| **Requirement** | The system shall be able to identify and classify SMS messages as spam or non-spam. |
| **Source** | System |
| **Rationale** | To protect users from unwanted SMS spam. |
| **Business Rule (if required)** | The system shall use a machine learning algorithm to classify SMS messages. |
| **Dependencies** | None |
| **Priority** | High |

**Functional Requirement Table 3**

|  |  |
| --- | --- |
| **Identifier** | FR-3 |
| **Title** | Spam Reporting |
| **Requirement** | The user shall be able to report an SMS message as spam. |
| **Source** | User |
| **Rationale** | To provide feedback to the system and improve its spam filtering accuracy. |
| **Business Rule (if required)** | The user shall click on a "Report Spam" button next to the SMS message. |
| **Dependencies** | None |
| **Priority** | Medium |

**Functional Requirement Table 4**

|  |  |
| --- | --- |
| **Identifier** | FR-4 |
| **Title** | Spam Filtering Accuracy |
| **Requirement** | The system shall have a spam filtering accuracy of at least 95%. |
| **Source** | System |
| **Rationale** | To ensure that the system is effective at filtering spam. |
| **Business Rule (if required)** | The system shall be tested on a large dataset of SMS messages to measure its spam filtering accuracy. |
| **Dependencies** | None |
| **Priority** | High |

**Functional Requirement Table 5**

|  |  |
| --- | --- |
| **Identifier** | FR-5 |
| **Title** | False Positives |
| **Requirement** | The system shall minimize false positives, which are non-spam messages that are incorrectly classified as spam. |
| **Source** | System |
| **Rationale** | To avoid inconveniencing users by blocking non-spam messages. |
| **Business Rule (if required)** | The system shall be tuned to minimize false positives without sacrificing spam filtering accuracy. |
| **Dependencies** | FR4 |
| **Priority** | High |

**Functional Requirement Table 6**

|  |  |
| --- | --- |
| **Identifier** | FR-6 |
| **Title** | User Interface |
| **Requirement** | The system shall have a user-friendly interface that allows users to easily submit SMS messages, view spam filtering results, and report spam. |
| **Source** | System |
| **Rationale** | To make the system easy to use for all users. |
| **Business Rule (if required)** | The system shall have a clear and concise interface with intuitive navigation. . |
| **Dependencies** | None |
| **Priority** | Medium |

**Functional Requirement Table 7**

|  |  |
| --- | --- |
| **Identifier** | FR-7 |
| **Title** | Performance |
| **Requirement** | The system shall be able to filter SMS messages quickly and efficiently. |
| **Source** | System |
| **Rationale** | To ensure that the system can handle the volume of SMS messages received. |
| **Business Rule (if required)** | The system shall be able to filter SMS messages in real time. |
| **Dependencies** | None |
| **Priority** | Medium |

**Functional Requirement Table 8**

|  |  |
| --- | --- |
| **Identifier** | FR-8 |
| **Title** | Security |
| **Requirement** | The system shall be secure and protect user data from unauthorized access. |
| **Source** | System |
| **Rationale** | To protect user privacy and prevent spammers from accessing the system. |
| **Business Rule (if required)** | The system shall implement appropriate security measures, such as user authentication and data encryption. |
| **Dependencies** | None |
| **Priority** | High |

**Functional Requirement Table 9**

|  |  |
| --- | --- |
| **Identifier** | FR-9 |
| **Title** | Machine Learning Model Training |
| **Requirement** | The system shall be able to train a machine learning model using a dataset of labeled SMS messages. |
| **Source** | System |
| **Rationale** | To enable the system to learn from past data and improve its spam filtering accuracy over time. |
| **Business Rule (if required)** | The dataset of labeled SMS messages must be representative of the types of messages that the system will encounter in real-world use. |
| **Dependencies** | None |
| **Priority** | High |

**Functional Requirement Table 10**

|  |  |
| --- | --- |
| **Identifier** | FR-10 |
| **Title** | Machine Learning Model Selection |
| **Requirement** | The system shall be able to select the most appropriate machine learning algorithm for the task of spam filtering. |
| **Source** | System |
| **Rationale** | To ensure that the system is using the most effective algorithm for filtering SMS spam. |
| **Business Rule (if required)** | The system shall select the machine learning algorithm that achieves the highest spam filtering accuracy on a validation dataset. |
| **Dependencies** | FR9, FR4 |
| **Priority** | High |

**Functional Requirement Table 11**

|  |  |
| --- | --- |
| **Identifier** | FR-11 |
| **Title** | Machine Learning Model Monitoring |
| **Requirement** | The system shall be able to monitor the performance of the machine learning model and retrain it as needed. |
| **Source** | System |
| **Rationale** | To maintain the accuracy of the system as the types of SMS spam evolve. |
| **Business Rule (if required)** | The system shall monitor the spam filtering accuracy of the machine learning model and retrain it if the accuracy falls below a certain threshold. |
| **Dependencies** | FR9, FR4 |
| **Priority** | High |

**Non Functional Requirements:**

* **Performance:**

The system shall be able to filter SMS messages in real time to ensure that users do not experience any delays in receiving or sending SMS messages.

* **Scalability:**

The system shall be able to handle the volume of SMS messages received to ensure that the system can scale to meet the needs of a growing user base.

* **Availability:**

The system shall be available 99.9% of the time to ensure that users are always able to use the system to filter their SMS messages.

* **Security:**

The system shall be secure and protect user data from unauthorized access to protect user privacy and prevent spammers from accessing the system.

* **Usability:**

The system shall have a user-friendly interface that allows users to easily submit SMS messages, view spam filtering results, and report spam to make the system easy to use for all users.

* **Maintainability:**

The system shall be easy to maintain and update to ensure that the system can be easily updated with new features and bug fixes.

* **Reliability:**

The system shall be reliable and able to handle errors gracefully to ensure that users can always rely on the system to filter their SMS messages correctly.

* **Compatibility:**

The system shall be compatible with a variety of mobile devices and operating systems to ensure that the system can be used by all users, regardless of their device or operating system.

* **Accuracy:**

The system shall achieve a spam filtering accuracy of at least 95% to ensure that the system effectively filters spam messages.

* **False Positivesl:**

The system shall minimize false positives, which are instances where legitimate SMS messages are incorrectly classified as spam, to ensure that users do not miss important messages.

* **False Negatives:**

The system shall minimize false negatives, which are instances where spam SMS messages are incorrectly classified as non-spam, to ensure that users are protected from unwanted spam messages.

* **Learn Rate:**

The system shall have a high learn rate, meaning that it can quickly adapt to new spam patterns and techniques, to maintain high spam filtering accuracy over time.

* **User Feedback:**

The system shall incorporate user feedback to improve spam filtering accuracy and identify new spam patterns.

* **Reporting:**

The system shall provide users with a mechanism to report spam messages, which can be used to refine the spam filtering algorithm.

* **Analytics:**

The system shall provide analytics to track spam filtering performance, identify trends, and inform future improvements.

|  |  |  |  |
| --- | --- | --- | --- |
| **Non-Functional Requirement** | **Description** | **Rationale** | **Priority** |
| **Performance** | The system shall be able to filter SMS messages in real time. | To ensure that users do not experience any delays in receiving or sending SMS messages. | High |
| **Scalability** | The system shall be able to handle the volume of SMS messages received. | To ensure that the system can scale to meet the needs of a growing user base. | Medium |
| **Availability** | The system shall be available 99.9% of the time. | To ensure that users are always able to use the system to filter their SMS messages. | High |
| **Security** | The system shall be secure and protect user data from unauthorized access. | To protect user privacy and prevent spammers from accessing the system. | High |
| **Usability** | The system shall have a user-friendly interface that allows users to easily submit SMS messages, view spam filtering results, and report spam. | To make the system easy to use for all users. | Medium |
| **Maintainability** | The system shall be easy to maintain and update. | To ensure that the system can be easily updated with new features and bug fixes. | Medium |
| **Reliability** | The system shall be reliable and able to handle errors gracefully. | To ensure that users can always rely on the system to filter their SMS messages correctly. | High |
| **Compatibility** | The system shall be compatible with a variety of mobile devices and operating systems. | To ensure that the system can be used by all users, regardless of their device or operating system. | Medium |

**Usability:**

* **Ease of Learning:**

**Simple and Intuitive Interface:** The system should have a simple and intuitive interface that is easy to understand and navigate, even for users with no prior experience with spam filtering tools.

**Clear Instructions and Prompts:** Clear and concise instructions and prompts should guide users through the various tasks and functionalities of the system, from submitting SMS messages for filtering to viewing spam classification results and reporting spam messages.

**Consistent Design:** The system should maintain a consistent design throughout, using similar layouts, terminology, and iconography to promote familiarity and reduce cognitive load.

* **Ease of Use:**

**Effortless SMS Submission:** Users should be able to submit SMS messages for spam filtering effortlessly, using various methods such as a web interface, mobile app, or SMS gateway integration. The system should handle various message formats and lengths without requiring users to manually adjust or convert messages.

**Straightforward Spam Filtering Results:** Spam filtering results should be presented in a clear and straightforward manner, allowing users to quickly identify spam and non-spam messages. Additional information, such as confidence scores and contributing factors, should be provided in a concise and understandable format.

**Simple Spam Reporting:** Reporting spam messages should be a simple and accessible process, requiring a single click or tap to initiate the reporting process. Users should be able to provide additional details about the spam message without being overwhelmed by unnecessary fields or complex instructions.

* **Error Avoidance and Recovery:**

**Error Prevention Mechanisms:** The system should implement mechanisms to prevent common errors, such as submitting empty messages or invalid formats. These mechanisms could include input validation, predictive text suggestions, and clear error messages.

**Informative Error Messages:** When errors do occur, the system should provide clear and informative error messages that explain the error and suggest corrective actions. Error messages should be free of jargon and technical terms, using plain language that is easy to understand.

**Easy Error Recovery:** Users should be able to easily recover from errors without losing data or progress. The system should provide undo/redo functionality, clear recovery instructions, and a mechanism to report persistent errors to the developers.

* **Efficiency of Interactions:**

**Quick and Responsive Interface:** The system should provide a quick and responsive interface that minimizes waiting times and allows users to complete tasks efficiently. This includes prompt loading times, smooth transitions between screens, and efficient message processing.

**Minimal User Input:** The system should minimize the amount of user input required to complete tasks. This could involve using pre-filled forms, automatic message categorization, and intelligent suggestions based on user behavior.

**Streamlined Submission and Reporting:** The processes of submitting SMS messages for filtering and reporting spam messages should be streamlined and efficient, allowing users to complete these tasks quickly and without unnecessary steps.

* **Accessibility:**

**WCAG 2.1 Compliance:** The system should comply with relevant accessibility standards, such as WCAG 2.1, to ensure that it is accessible to users with disabilities, including visual, auditory, or motor impairments.

**Alternative Input and Output Methods:** The system should provide alternative input and output methods for users with different needs, such as screen readers, keyboard navigation, and voice control.

**High-Contrast Color Schemes:** High-contrast color schemes and adjustable text sizes should be available to accommodate users with visual impairments.

**Clear Auditory Feedback:** Clear and concise auditory feedback should be provided for users with hearing impairments.

**Multilingual Support:** The system should support multiple languages to cater to a global user base. Users should be able to easily change the language of the user interface from a dedicated menu or settings page

**Performance:**

* **Processing Speed:**

**Requirement:** The system should process incoming SMS messages in real-time.

**Performance Goal:** Achieve a processing speed of at least 1000 messages per second.

* **Latency:**

**Requirement:** The system should provide low-latency response for spam classification.

**Performance Goal:** Maintain an average latency of less than 100 milliseconds for spam detection.

* **Accuracy:**

**Requirement:** The system should accurately identify spam messages.

**Performance Goal:** Achieve a spam detection accuracy of at least 98%.

* **Scalability:**

**Requirement:** The system should handle a growing volume of SMS messages.

**Performance Goal:** Scale horizontally to support a 50% increase in message volume without significant degradation in performance.

* **Resource Utilization:**

**Requirement:** The system should use system resources efficiently.

**Performance Goal:** Ensure CPU utilization stays below 70% and memory usage below 80% during peak processing times.

* **Training Speed:**

**Requirement:** The system should be able to adapt to new spam patterns efficiently.

**Performance Goal:** Achieve a training speed of processing 1000 training samples in less than 5 minutes.

* **False Positive Rate:**

**Requirement:** Minimize false positives to avoid blocking legitimate messages.

**Performance Goal:** Maintain a false positive rate below 1%.

* **False Negative Rate:**

**Requirement:** Minimize false negatives to ensure effective spam filtering.

**Performance Goal:** Keep the false negative rate below 2%.

* **User Interface Responsiveness:**

**Requirement:** The user interface for managing spam settings should be responsive.

**Performance Goal:** Ensure that user interface interactions have a response time of less than 300 milliseconds.

* **Logging and Auditing:**

**Requirement:** The system should maintain logs for auditing and analysis.

**Performance Goal:** Log generation should not impact system performance, with log entries processed in real-time.

**References:**

<https://sist.sathyabama.ac.in/sist_naac/documents/1.3.4/1822-b.e-cse-batchno-109.pdf>

<https://worldwidescience.org/topicpages/s/sms+spam+filtering.html>

<https://bard.google.com/chat/bfd286e1f35d3cfe>

<https://chat.openai.com/c/283728a4-2a0f-4be6-a870-b98f7d1b83db>

<https://chat.openai.com/c/775ae04a-f57b-44ed-b98a-bdb9b7b18792>

<https://chat.openai.com/c/ca3bec73-16b4-4461-8614-07cfde322d93>

<https://chat.openai.com/c/5609a0c3-e898-4935-b4fc-56fd4c981e37>

<https://chat.openai.com/c/dcf137d1-000c-481e-8d15-f4b4f3df1e00>

<https://chat.openai.com/c/379e0a02-796e-4a03-b910-04906433b011>

<https://bard.google.com/chat/bfd286e1f35d3cfe>