Aegis Secure – Use Cases

IT314 - Software Engineering

Group - 35

❖ Introduction

This document outlines the key use cases implemented in the Aegis Secure application. Each use case describes how the user interacts with the system, the conditions required for the interaction and the sequence of steps followed by both the user and the system.

The document includes the goals, actors, pre-conditions, post-conditions, main flow and alternate flows for each feature. The use cases presented here provide a clear and structured understanding of the system's functional behaviour.

➢ UC-01: User Registration

Goal:
Allow a new user to create an account and verify it using OTP.

Primary Actor:
User

Pre-conditions:

- User is not already registered.

Post-conditions:

- User account is created in the system.
- OTP is sent to the user for verification.
- User is verified after entering correct OTP.

Main Flow:

1. User opens the app and navigates to the registration screen.
2. User enters name, email and password.
3. User clicks on the “i” icon, system displays the password strength requirements.
4. User agrees to the Terms and Conditions.
5. User clicks on the Sign Up button.
6. System checks if the email already exists.
7. System checks if password meet the requirements.
8. System creates a new user account.
9. System sends an OTP to the user’s email.
10. User enters the OTP in the app.
11. System verifies the OTP.
12. System confirms account verification.

Alternate Flows:
2a. User has not entered name/email/password, system shows “Please enter your name/email/password.”
4a. User does not agree to the Terms and Conditions, system shows “Please agree to the terms & conditions.”
6a. Email already exists, system shows “This Email is Already Registered!”
7a. Password requirements do not meet, system shows “Password does not meet all requirements”
10a. User clicks on Resend OTP.
11b. User enters an invalid or expired OTP, system shows “Invalid or expired OTP. Please try again.”

➢ UC-02: User Login

Goal:
Allow a verified user to log in securely using email and password.

Primary Actor:
User

Pre-conditions:

- User must be registered.
- User must have completed OTP verification.

Post-conditions:

- User is successfully logged in and receives an authentication token.
- User can access all app features.

Main Flow:

1. User opens the app and navigates to the login screen.
2. User enters email and password.
3. User clicks on the Sign In button.
4. System validates the email and password.
5. System verifies that the user is already OTP-verified.
6. System logs the user in.

Alternate Flows:
2a. User has not entered email/password, system shows “Enter the email/password.”
4a. Email or password is incorrect, system shows “Invalid email or password.”
5a. User has not completed OTP verification, system shows “Please verify your email before logging in.”

➢ UC-03: Auto Scan Gmail

Goal:
Automatically scan Gmail emails using the ML model.

Primary Actor:
User

Secondary Actors:
Aegis Secure backend system with ML model, Google Gmail API

Pre-conditions:

- User is logged in.
- User has connected a Gmail account.
- Required Gmail permissions are granted.
- Auto Gmail scan is enabled in settings.

Post-conditions:

- New Gmail emails are scanned and results are stored.

Main Flow:

1. User connects Gmail account from the app.
2. System uses the Gmail API to fetch new emails for the connected account.
3. System extracts sender, subject and body from each new email.
4. System sends the extracted data to the ML model for analysis.
5. ML model returns scan results such as safe or scam with confidence score and other results.
6. System stores the results and updates the dashboard data.
7. User opens the specific email for highlighted risks, reasoning and suggestion.

Alternate Flows:
3b. No new emails are available, system does nothing and waits for the next interval.
4a. ML model service is unavailable, system retry scanning later.

➢ UC-04: Auto Scan SMS

Goal:
Automatically scan SMS messages on the device using the ML model.

Primary Actor:
User

Secondary Actor:
Aegis Secure backend system with ML model

Pre-conditions:

- User is logged in.
- SMS read permission is granted.
- Auto SMS scan is enabled in settings.

Post-conditions:

- New SMS messages are scanned and results are stored.

Main Flow:

1. User opens settings and enables auto SMS scan.
2. System checks the device for new SMS messages.
3. System extracts sender and message body for each new SMS.
4. System sends the extracted data to the ML model for analysis.
5. ML model returns scan results such as safe or scam with confidence score and other results.
6. System stores the results and updates the dashboard data.
7. User opens the specific SMS for highlighted risks, reasoning and suggestion.

Alternate Flows:
3a. No new SMS messages are available, system does nothing and waits for the next interval.
4a. ML model service is unavailable, system retry scanning later.

➢ UC-05: Manual Text Input Scan

Goal:
Allow the user to manually enter any text and check if it is a scam using the ML model.

Primary Actor:
User

Secondary Actor:
Aegis Secure backend system with ML model

Pre-conditions:

- User is logged in.
- ML model API is accessible.

Post-conditions:

- The entered text is analysed and the result is shown to the user.

Main Flow:

1. User opens the manual text analysis screen in the app.
2. User enters text into the text box.
3. User taps the analyse button.
4. System sends the text to the ML model for score.
5. ML model returns the score, system displays the prediction result to the user.

Alternate Flows:
3a. Text box is empty when user taps analyse button, system waits for user to enter the text.

➢ UC-06: View Dashboard

Goal:
Allow the user to view the statistics of scanned SMS and emails.

Primary Actor:
User

Pre-conditions:

- User is logged in.

Post-conditions:

- Updated dashboard information is shown to the user.

Main Flow:

1. User opens the dashboard screen.
2. System requests the latest dashboard data from the backend.
3. Backend returns the most recent dashboard information.
4. User selects SMS, Email or Both to view the corresponding statistics.
5. System displays the selected statistics along with cyber insights.

Alternate Flows:
2a. No new dashboard data is available, system does nothing and waits for next intervals.