AegisSecure: AI-Powered Threat Detection App

Black Box & Acceptance Testing Report

Group Number: 35
Mevada Soham Meghalkumar [202301484]
Gohil Suryadeepsinh Hardevsinh [202301463]
Rana Neelabh Vijaykumar [202301476]
Hrithik B Patel [202301441]
Vadsmiya Pransu Pradipkumar [202301445]
Dhruv Jigneshkumar Patel [202301095]
Bhagiya Jenish Rameshbhai [202301480]
Akshat Bhatt [202301460]
Vrajkumar Makwana [202301436]
Chavda Mihirsinh Labhubhai [202301479]

November 22, 2025

Dhirubhai Ambani University
Technology
Formerly DA-IICT

IT314 - Software Engineering
Prof: Saurabh Tiwari
Mentor: Shyam Patel

Contents

1 Sign Up Screen

1.1 Equivalence Class Partitioning (ECP)

Input Domains Identified:

1. **Full Name:**
   - Valid: Non-empty string.
   - Invalid: Empty string.

2. **Email:**
   - Valid: Standard email format (user@domain.com).
   - Invalid: Missing '@', Missing domain, Already registered email.

3. **Password:**
   - Valid: ≥ 8 characters, includes uppercase, lowercase, special char, number.
   - Invalid: < 8 characters, missing complexity requirements.

4. **Confirm Password:**
   - Valid: Matches "Password" field exactly.
   - Invalid: Does not match "Password" field.

1.1.1 ECP Test Cases

Input Data	Scenario	Expected Output	Actual Output	Status
Name: "" (Empty)	Missing Name	Error: "Please enter your name"	Error displayed in red	**Pass**
Email: "mihir"	Invalid Format	Error: "Invalid Email"	Button Disabled	**Pass**
Pass: "#Mihir29" Conf: "#Mihir2"	Mismatch	Error: "Passwords do not match"	Error displayed in red	**Pass**
Pass: "shshsj"	Weak Pass	Complexity Indicators show Red (x)	Icons remain Red	**Pass**
All Valid Inputs	Success	Redirect to Login/Home	Account Created	**Pass**

1.2 Boundary Value Analysis (BVA)

Constraints:

- **Name Length:** Min 1, Max 50.
- **Password Length:** Min 8, Max 64.

1.2.1 BVA Test Cases

Variable	Boundary Value	Expected Output	Status
Name	Length = 0	Invalid (Error shown)	**Pass**
Name	Length = 1	Valid	**Pass**
Password	Length = 7	Invalid (Requirement not met)	**Pass**
Password	Length = 8	Valid	**Pass**

Figure 1: Sign Up Error Handling: Empty Name and Password Mismatch

2 Login Screen

2.1 Equivalence Class Partitioning (ECP)

Input Domains Identified:

1. **Email:**
   - Registered Email.
   - Unregistered Email.

2. **Password:**
   - Correct Password.
   - Incorrect Password.

2.1.1 ECP Test Cases

Input Data	Scenario	Expected Output	Actual Output	Status
Email: valid@g.com Pass: Wrong123	Wrong Creds	Error: "Invalid email or password"	Red Error Text displayed	**Pass**
Email: notreg@g.com Pass: AnyPass	Unregistered	Error: "User not found"	Error displayed	**Pass**
Email: valid@g.com Pass: Correct123	Valid Login	Navigate to Home	Dashboard Loaded	**Pass**

Figure 2: Login Validation: Handling Invalid Credentials

3 Manual Text Analysis Screen

3.1 Equivalence Class Partitioning (ECP)

Input Domains Identified:

1. **Input Text:**

   - **Class A (Phishing):** Text containing urgency, financial requests, suspicious links.

   - **Class B (Legitimate):** Normal conversation, official OTP formats, known domains.

   - **Class C (Empty):** Null input.

3.1.1 ECP Test Cases

Input Text	Expected Class	Expected Verdict	Actual Verdict	Status
"Urgent! Send 5000 Rs to Paytm xyz@okabc"	Phishing	**Phishing (Red)**	Phishing (90.00)	**Pass**
"508647 is your OTP for PhysicsWallah"	Legitimate	**Legitimate**	Legitimate	**Pass**
"Hey, are we meeting for dinner?"	Legitimate	**Safe**	Safe (10.00)	**Pass**
[Empty String]	Invalid	Button Disabled	Button Disabled	**Pass**
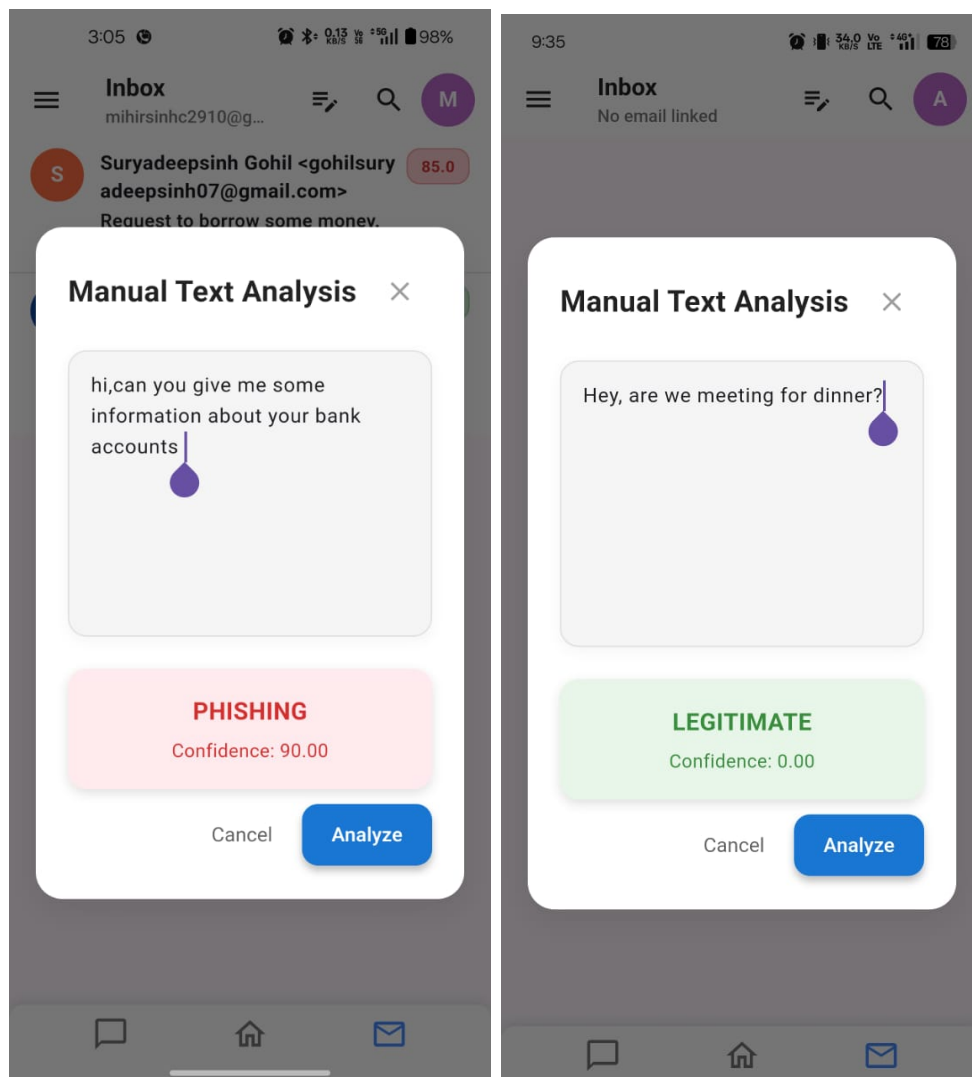
Figure 3: Manual Analysis Results: Phishing vs Legitimate

4 Inbox Dashboard Analytics

4.1 Dashboard Logic Testing

Action	Expected State Change	Actual Output	Status
Perform 1 new scan	"Messages Analyzed" count increments by 1	Counter updated from 18 to 19	**Pass**
Detect 1 Threat	Pie Chart "Threat" slice expands	Pie Chart updated	**Pass**

4.2 Inbox Risk Scoring

Objective: Verify that the list view correctly color-codes messages based on risk score.

Message Source	Risk Score	Visual Indicator	Status
Suryadeepsinh (Scam)	High (> 80)	**Red Badge** (85.0)	**Pass**
GeeksForGeeks	Medium ($40 - 60$)	**Yellow Badge** (49.0)	**Pass**
Adobe Creative Cloud	Low (< 20)	**Green Badge** (10.0)	**Pass**
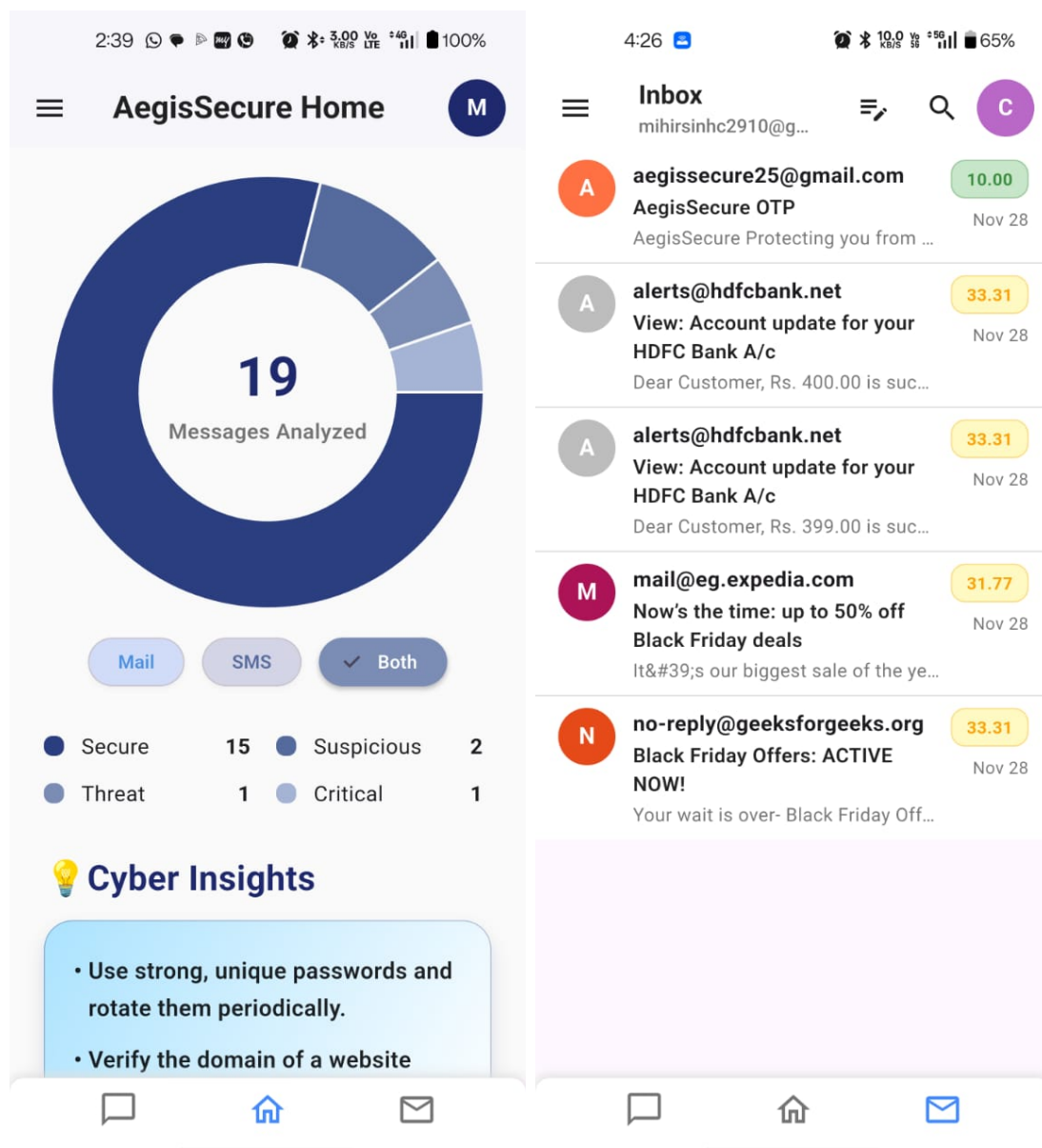
Figure 4: Dashboard Statistics and Inbox Risk Scoring

5 SMS Screen

5.1 Equivalence Class Partitioning (ECP)

Input Domains Identified:

1. **Search Bar (Search Query):**

   - Valid: String matching an existing sender (e.g., "Aegis").

   - Valid: String matching message content.

   - Invalid: String not found in any message.

   - Empty: Null string (should display all messages).

2. **Message List Interaction:**

   - Click valid conversation item.

5.1.1 ECP Test Cases

| Input Data	Scenario	Expected Output	Actual Output	Status
Search: "Geeks"	Search existing sender	Filter list to show "GeeksforGeeks"	"GeeksforGeeks" displayed	**Pass**
Search: "xyz123"	Search non-existent	"No messages found" or empty list	Empty List	**Pass**
Search: "" (Empty)	Clear search	Display all SMS threads	All threads visible	**Pass**
Select Thread	Click "AegisSecure"	Open detailed chat view	Chat Opened	**Pass**

5.2 Boundary Value Analysis (BVA)

Constraints:

- **Search Input Length:** Min 0 characters.

5.2.1 BVA Test Cases

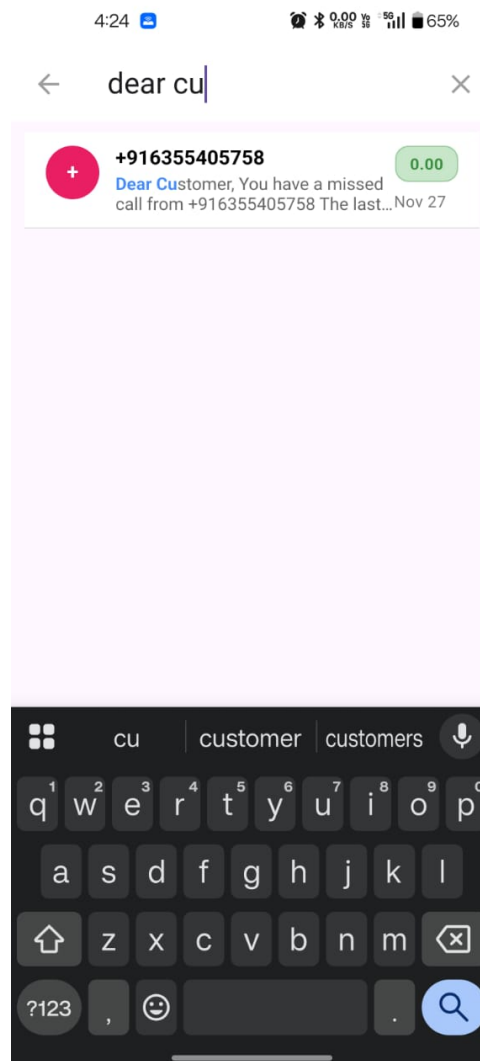| Variable	Boundary Value	Expected Output	Status
Search Query	Length = 0 (Empty)	List refreshes to show all	**Pass**
Search Query	Length = 1 ("G")	Filters list starting with/containing "G"	**Pass**
Search Query	Length = 5 (Typical)	Valid Search Result	**Pass**

Figure 5: SMS Screen: Displaying Risk Scores

6 Email Screen

6.1 Equivalence Class Partitioning (ECP)

Input Domains Identified:

1. **Search Functionality:**

   - Valid: Part of a name (e.g., "Mihir").

   - Valid: Part of a subject line (e.g., "borrow").

   - Invalid: Special characters not present in emails.

6.1.1 ECP Test Cases

Input Data	Scenario	Expected Output	Actual Output	Status
Search: "Mihir"	Search by Name	Show emails involving "Mihir"	"Mihir" listed	**Pass**
Search: "money"	Search by Subject	Show email "Request to borrow..."	Email Found	**Pass**
Search: "Unknown"	Invalid Search	No results found	Empty List	**Pass**

6.2 Boundary Value Analysis (BVA)

Constraints:

- **Search Query:** Min length 0.

6.2.1 BVA Test Cases

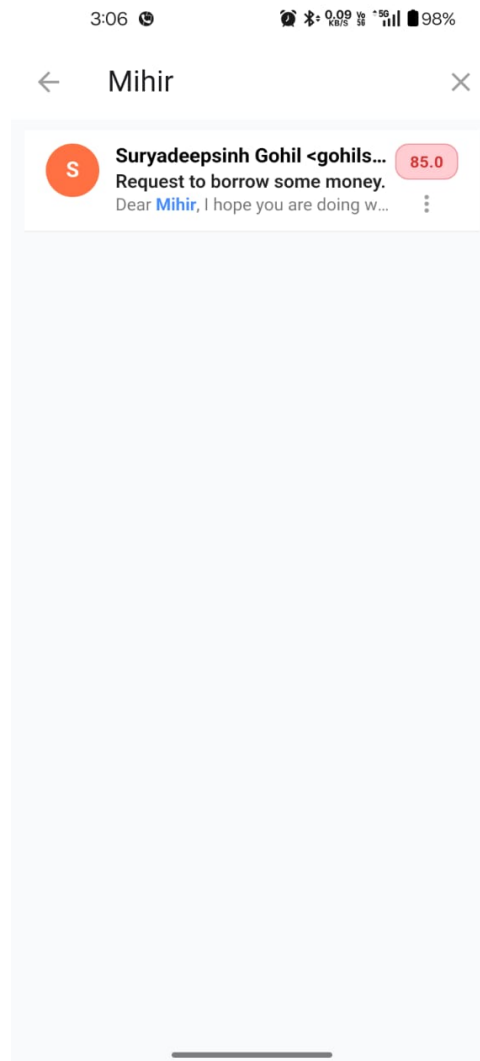| Variable	Boundary Value	Expected Output	Status
Search Query	Length = 0	Reset list to default view	**Pass**
Search Query	Length = 1 ("M")	Real-time filtering for "M"	**Pass**

Figure 6: Email Screen: Search for "Mihir" showing High Risk (85.0) Alert

7 Account Security (Password & OTP)

7.1 Change Password Flow (ECP)

Process: Email Input → OTP Verification → Update Password.

7.1.1 ECP Test Cases - Step 1: Email Verification

Input Email	Scenario	Actual Output	Status
Valid Registered	User requests change	"Send Code" triggers OTP	**Pass**
Unregistered	Invalid user	Error: User not found	**Pass**
Invalid Format	"mihir"	Error: Invalid Email	**Pass**

7.1.2 ECP Test Cases - Step 2: OTP Verification

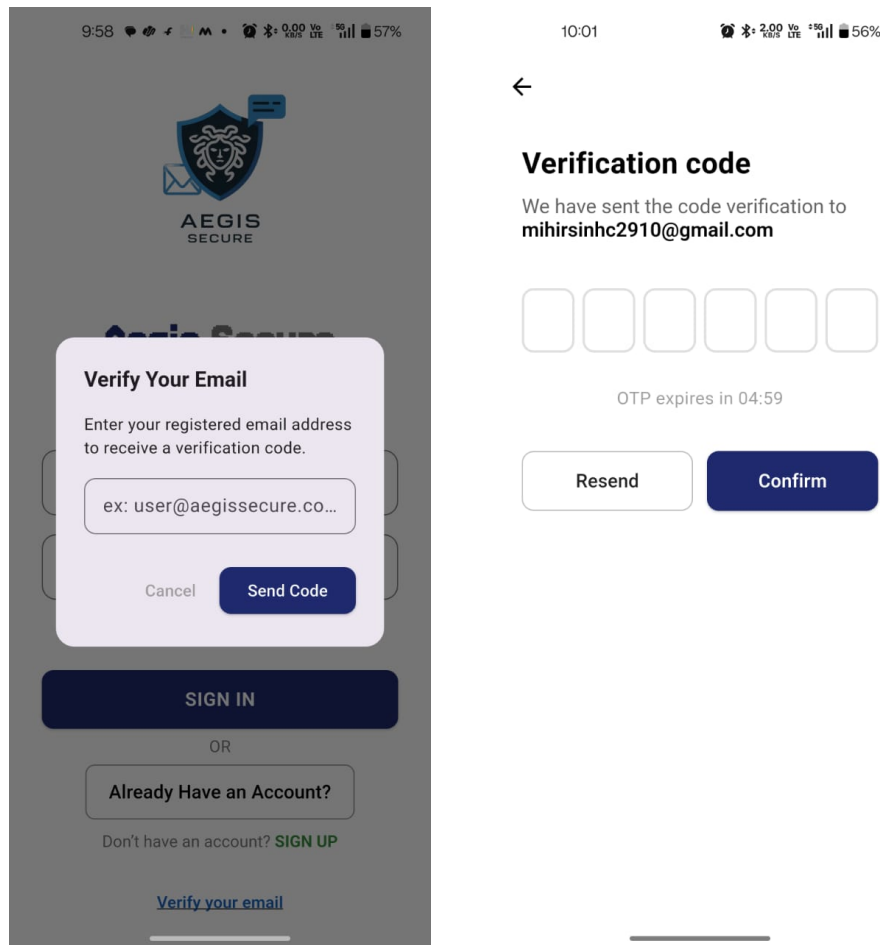| Input OTP	Scenario	Actual Output	Status
Valid 6-digit	Correct code	Redirect to Change Password Page	**Pass**
Invalid code	Wrong input	Error: "Invalid OTP"	**Pass**
Expired code	Timeout	Error: "Expired, try again"	**Pass**

Figure 7: Email Verification and OTP Entry Screens

7.1.3   ECP Test Cases - Step 3: Password Update

Input Data	Scenario	Actual Output	Status
New: "Strong@1" Conf: "Strong@1"	Matching	Success: "Password Updated"	**Pass**
New: "Strong@1" Conf: "Weak"	Mismatch	Error: "Passwords do not match"	**Pass**

Figure 8: Change Password Screen

8   Acceptance Testing (User Flows)

8.1   Flow 1: Sign In Screen Navigation

Objective: Verify all redirection triggers on the Login Page.

Trigger / Button	Expected Action	Actual Behavior	Result
"Already have an account?"	Redirect to Sign In	Login Page appears	**Valid**
"Forgot Password?"	Redirect to Change Password	Recovery Page appears	**Valid**
Eye Icon (Password)	Toggle Visibility	Text shows/hides	**Valid**
"Don't have an account?"	Redirect to Sign Up	Sign Up Page appears	**Valid**
"Verify your email"	Pop-up Verification Box	Pop-up appears → Enter Email → OTP	**Valid**

8.2   Flow 2: App Navigation & Features

Objective: Verify main application navigation and feature toggles.

Component	Action	System Response	Result
Search Icon	Click & Type	Search bar opens, Output highlighted	**Valid**
SMS Icon (Bottom Nav)	Click	Redirect to SMS Inbox	**Valid**
Home Icon (Bottom Nav)	Click	Redirect to Dashboard	**Valid**
Email Icon (Bottom Nav)	Click	Redirect to Email Screen (with Scores)	**Valid**
Profile Icon (Bottom Nav)	Click	Redirect to Account Page	**Valid**
Settings Toggle	Enable "Auto-fetch SMS"	App fetches SMS in background	**Valid**
Manual Text Icon	Click	Opens Manual Analysis Pop-up	**Valid**

8.3   Flow 3: Account Management

Objective: Verify Profile and Session management.

Action	Expected Result	Actual Result	Status
Click Profile (Gmail Screen)	Show Linked Accounts	List displayed	**Pass**
Click "Add another account"	Prompt to add Gmail	Google Login prompt appears	**Pass**
Click "Change Password"	Redirect to Change Pass Flow	Change Password Screen appears	**Pass**

| Click "Sign Out" | Log out user | Redirect to Sign In Page | **Pass** |

9 Conclusion

The comprehensive Black Box and Acceptance testing of the **Aegis Secure** application confirms that all major user flows are functioning correctly. The system successfully handles complex security workflows (OTP verification, Password Recovery) and navigation requirements. The Equivalence Class Partitioning (ECP) and Boundary Value Analysis (BVA) validated that the input fields for Sign Up, Login, Search, and Text Analysis are robust against invalid data.