AegisSecure: AI-Powered Threat Detection App

Combined Report (Sprint 1 — Sprint 4)

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]

Dhirubhai Ambani University
Technology

Formerly DA-IICT

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

Contents

Sprint 1 — Mid-Evaluation Report (POC & Requirements)

Requirements Elicitation

Multiple elicitation techniques were used to define scope and identify stakeholder needs:

- Brainstorming sessions within the team to refine vision and scope.
- A Google Form survey to collect quantitative user preferences.
- Focus groups to gather qualitative feedback across target demographics.
- Interviews with domain-aware participants to validate assumptions.
- Research of relevant APIs, platform constraints, privacy and regulatory considerations.

Stakeholders and Users

Key stakeholders and user groups identified:

- Individual end users (consumers).
- Email and SMS service providers (integration considerations).
- Cloud service providers (deployment and scaling).
- Dataset providers and data custodians (privacy and compliance).
- Cybersecurity experts and advisors.
- Development team and academic mentor.

Functional Requirements (summary)

Selected functional requirements identified during Sprint 1:

- FR-001 — Scam detection with binary label (Safe / Scam), confidence score and plain-language explanation.
- FR-002 — Result dashboard with recent scans, filters, sorting and risk categorization.
- FR-003 — Manual input (paste/type) with immediate scanning.
- FR-004 — Permissioned SMS/Email integration with explicit consent and audit logging.
- FR-005 — Background auto-scanning service with alerting.
- FR-006 — User feedback loop to collect labels for continuous improvement.
- FR-007 — Push notifications for flagged items.
- FR-008 — Secure user registration, password policy and verification.
- FR-009 — Settings and account preferences persisted per user.
- FR-010 — Multilingual analysis and graceful fallback behavior.
- FR-011 — Summary screen with history and visualization (pie chart).
- FR-012 — Multilingual UI support.

Non-Functional Requirements (summary)

Key non-functional requirements:

- NFR-001 — Privacy and data minimization: default behaviour avoids storing raw message bodies; only analysis metadata retained.
- NFR-002 — Secure connections and secrets management: TLS enforced and passwords stored using secure hashing.
- NFR-003 — Accuracy targets for detection models; confidence reporting.
- NFR-004 — Performance targets for latency on manual and auto scans.
- NFR-005 — Simplicity and accessibility of UI and explanations.

User Stories and Epics

User stories were created and grouped into epics for planning:

- Epic 1: Scam Detection & Analysis.
- Epic 2: User Interaction & Visualization.
- Epic 3: Input & Scanning Options.
- Epic 4: User Account & Personalization.
- Epic 5: Feedback & Continuous Improvement.
- Epic 6: Security & Privacy.

Sprint 1 Proof of Concept

Delivered items in Sprint 1:

- Wireframes and UI prototypes for core screens.
- Initial sign-up and sign-in implementation with verification flow.
- Baseline classification model capable of returning label and confidence.

Sprint 2 Report

Sprint Objective: Implement secure user registration and establish reliable email synchronization for spam/ham identification.
Duration (Planned): 22 September – 20 October
Time Spent (Actual): 22 September – 24 October

Summary: Sprint 2 focused on user registration, authentication and email fetching via Gmail API. The authentication flow and email synchronization were implemented as core deliverables. SMS access remained blocked by platform restrictions and was deferred.

Sprint Backlog (Sprint 2)

Below are the epics and user stories planned for Sprint 2 along with acceptance criteria.

Epic-2 : Secure User Registration

US-8: Secure User Registration

Front Card

As a new user, register with email/phone and a strong password to securely access the app.

Back Card

Success:

- Unique email/phone validation and password strength enforcement.
- Confirmation via email/SMS with verification link or OTP.
- User profile created with default settings.

Failure:

- Duplicate accounts allowed.
- Weak passwords accepted.
- Missing verification flow.

Epic-3 : Input & Scanning

US-3: Manual Input

Front Card

Allow pasting of suspicious text for manual scanning.

Back Card

Success:

- Manual input validated and processed.
- Results returned within acceptable latency.

Failure:

- Acceptance of empty input.
- No response or timeout.

US-4: SMS/Email Integration

Front Card

Implement secure SMS/email integration that runs with explicit permission.

Back Card

Success:

- Email/SMS access gated by user consent.

Failure:

- Access without consent.
- Failure to obtain access despite user consent.

US-5: Auto Scanning Service

Front Card

Provide a background service to scan incoming messages automatically.

Back Card

Success:

- Background scanning triggers alerts for suspicious items.
- Notifications present confidence and severity.

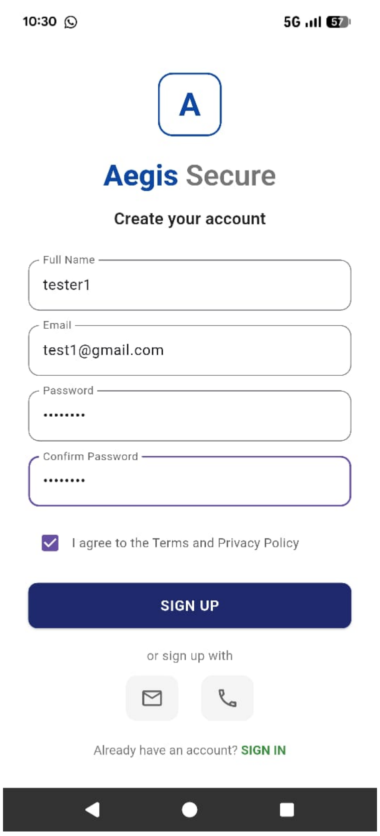
Failure:

- Auto-scan failures or missing alerts.

Sprint 2 — POC / Deliverables

User Authentication and Verification

Completed registration, sign-in and email verification flows with OTP verification.



Create your account

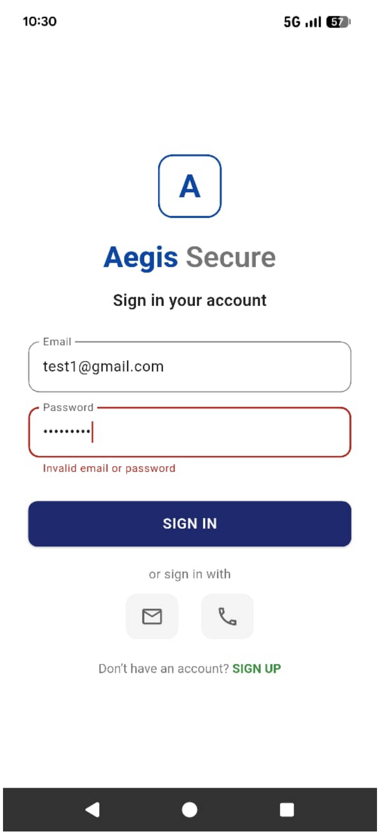
Full Name: tester1

Email: test1@gmail.com

Password: ••••••••

Confirm Password: ••••••••

☑ I agree to the Terms and Privacy Policy

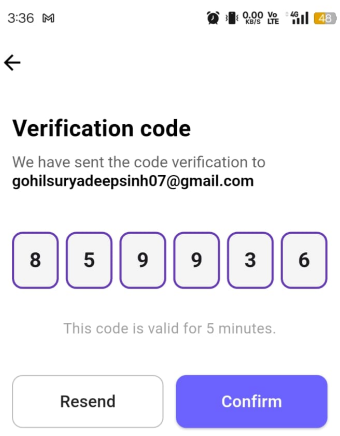


Sign in your account

Email: test1@gmail.com

Password: •••••••••

Invalid email or password



Verification code

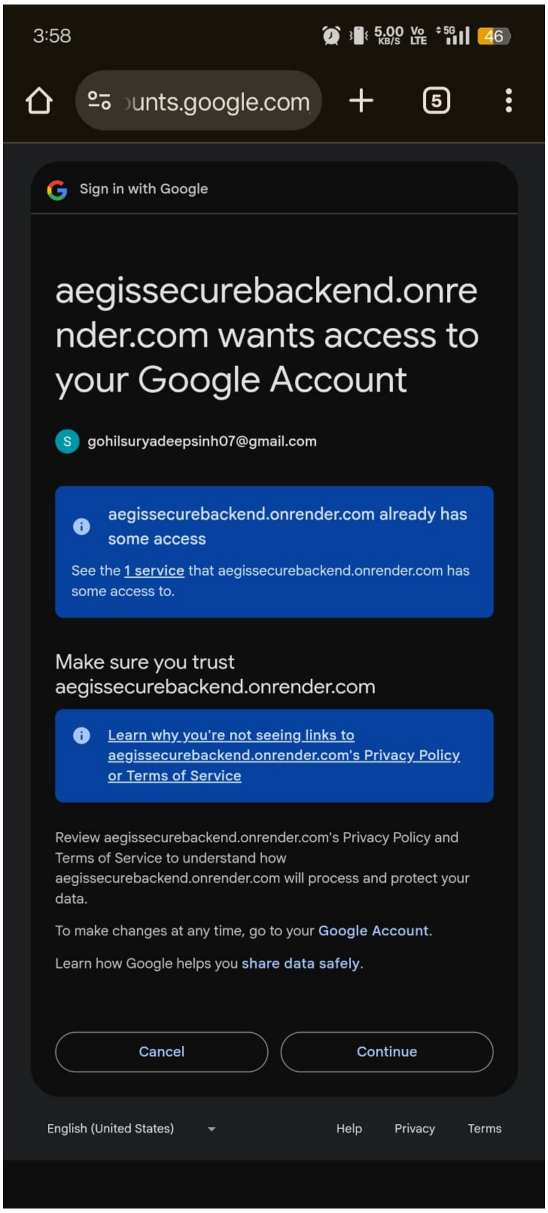
We have sent the code verification to gohilsuryadeepsinh07@gmail.com

8 5 9 9 3 6

This code is valid for 5 minutes.

Email Synchronization and Scoring

Google OAuth and Gmail API integrated; inbox view with per-email confidence score.



aegissecurebackend.onrender.com wants access to your Google Account

S gohilsuryadeepsinh07@gmail.com

aegissecurebackend.onrender.com already has some access

See the 1 service that aegissecurebackend.onrender.com has some access to.

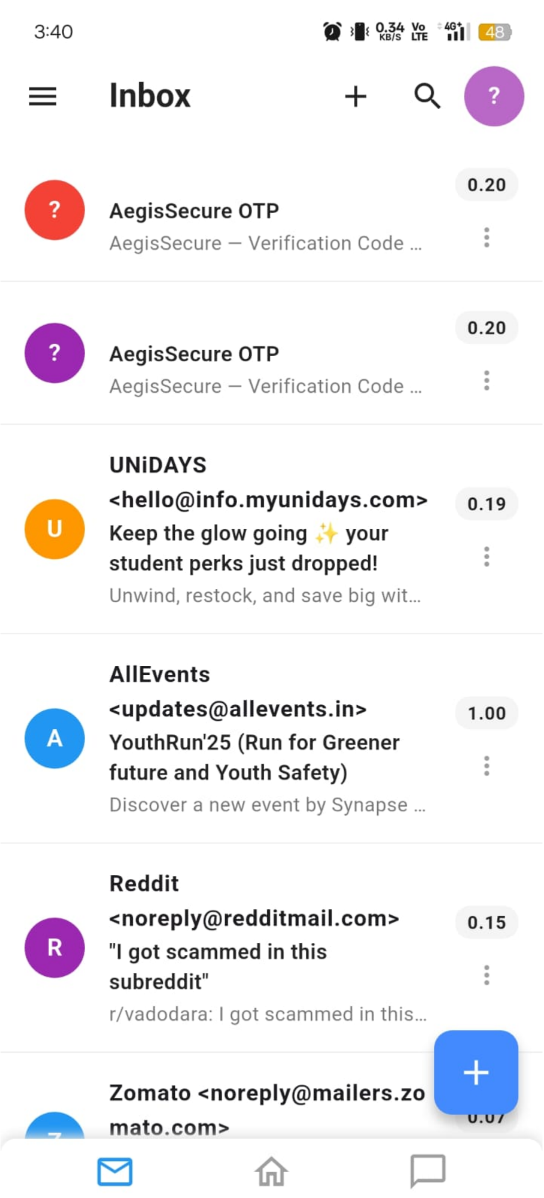
Make sure you trust aegissecurebackend.onrender.com

Learn why you're not seeing links to aegissecurebackend.onrender.com's Privacy Policy or Terms of Service

Review aegissecurebackend.onrender.com's Privacy Policy and Terms of Service to understand how aegissecurebackend.onrender.com will process and protect your data.

To make changes at any time, go to your Google Account.

Learn how Google helps you share data safely.



? AegisSecure OTP 0.20
AegisSecure — Verification Code ...

? AegisSecure OTP 0.20
AegisSecure — Verification Code ...

U UNiDAYS <hello@info.myunidays.com> Keep the glow going ✨ your student perks just dropped! 0.19
Unwind, restock, and save big wit...

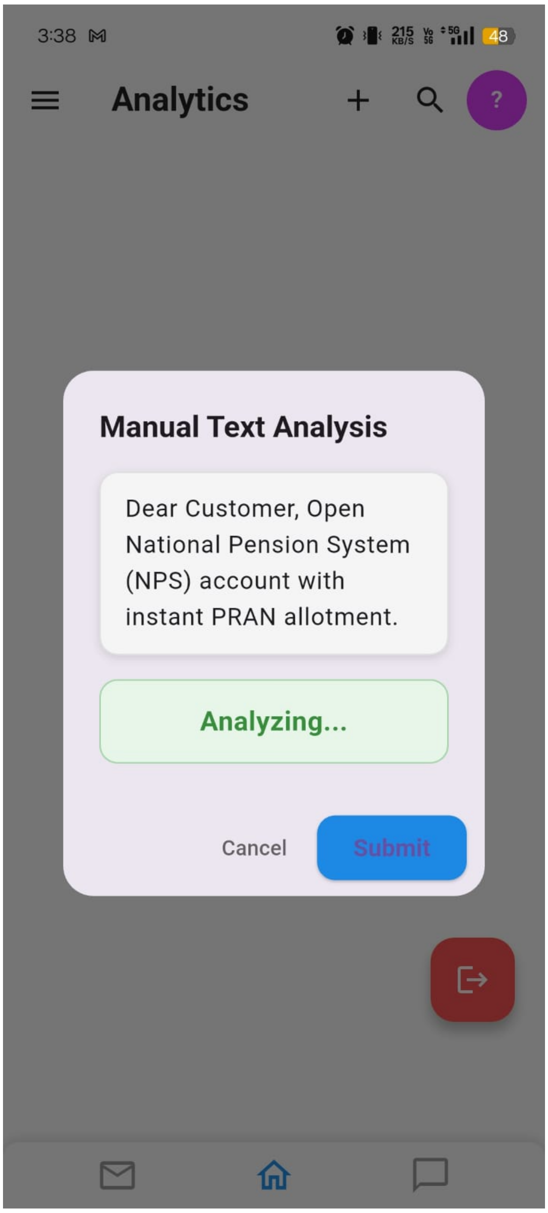
A AllEvents <updates@allevents.in> YouthRun'25 (Run for Greener future and Youth Safety) 1.00
Discover a new event by Synapse ...

R Reddit <noreply@redditmail.com> "I got scammed in this subreddit" 0.15
r/vadodara: I got scammed in this...

Z Zomato <noreply@mailers.zomato.com> 0.07

Manual Text Analysis

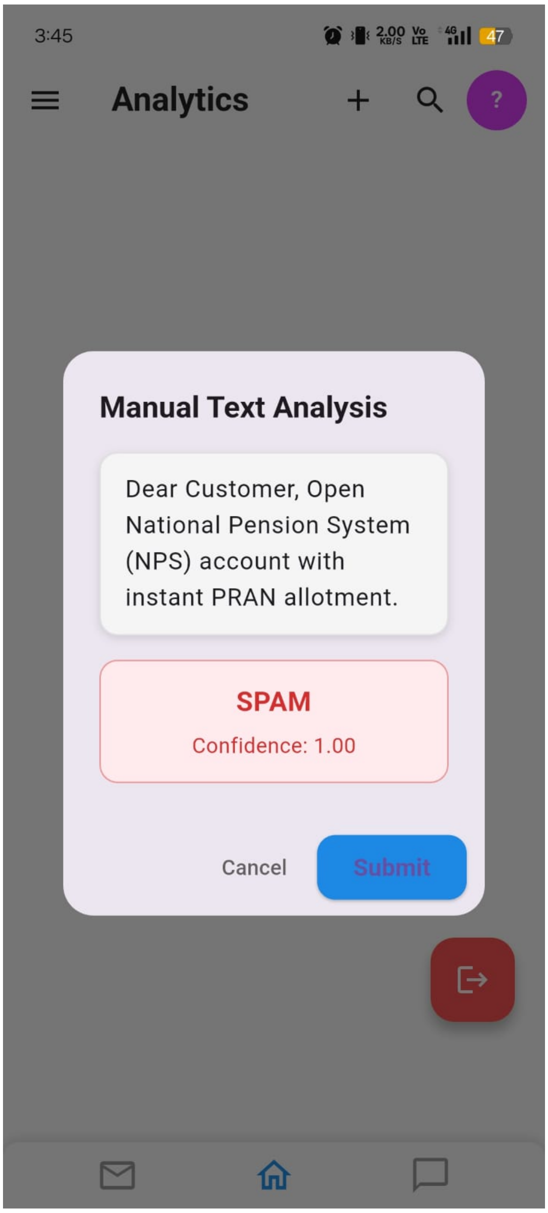
Manual text input and immediate analysis returning verdict and confidence.



Manual Text Analysis

Dear Customer, Open National Pension System (NPS) account with instant PRAN allotment.

Analyzing...



Manual Text Analysis

Dear Customer, Open National Pension System (NPS) account with instant PRAN allotment.

SPAM

Confidence: 1.00

Sprint 3 Report

Sprint Objective: Implement result visualization (dashboard, history), integrate the advanced detection model, and complete SMS/Email scanning.
Duration (Planned): 25 October – 7 November
Time Spent (Actual): 25 October – 10 November

Summary: Sprint 3 delivered the main user-facing visualization features, integration of a higher-accuracy detection model, and completion of the SMS fetching strategy that had blocked earlier progress.

Sprint Backlog (Sprint 3)

Epic-4 : Result Visualization & Simplicity

US-2: Result Dashboard

Front Card

Provide a dashboard that displays scan results and categorizes threats by risk level.

Back Card

Success:

- Clear presentation of results and confidence scores.

US-11: Summary Screen with History

Front Card

Provide a summary screen with a pie chart and history listing.

Epic-5 : Advanced Detection Quality

US-10: Multilingual Analysis

Front Card

Support analysis for multiple languages with fallbacks.

Back Card

Status: Implemented (initial translation + analysis logic; accuracy varies by language).

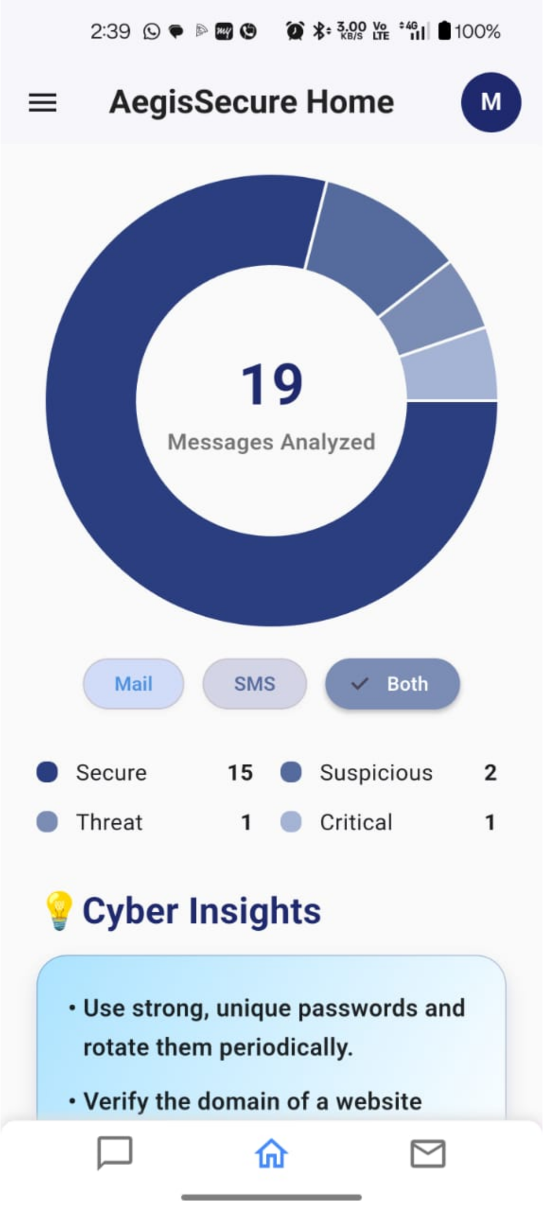
US-15: Accuracy

Front Card

Improve detection accuracy and reduce false positives/negatives.

Sprint 3 — POC / Deliverables

Summary Screen and Dashboards



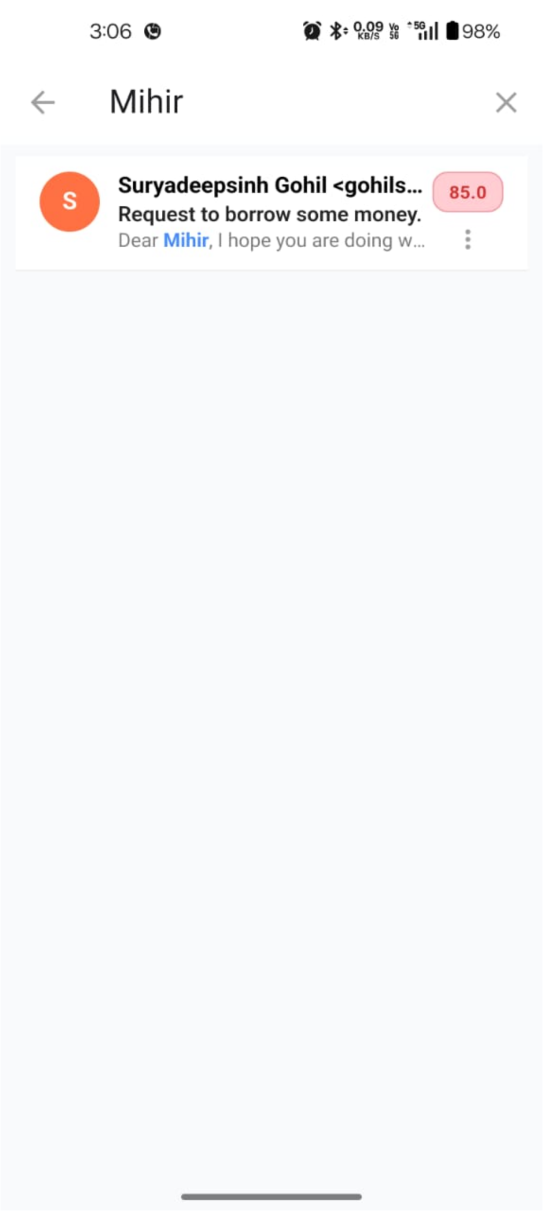
19

Messages Analyzed

● Secure	15	● Suspicious	2
● Threat	1	● Critical	1

💡 Cyber Insights

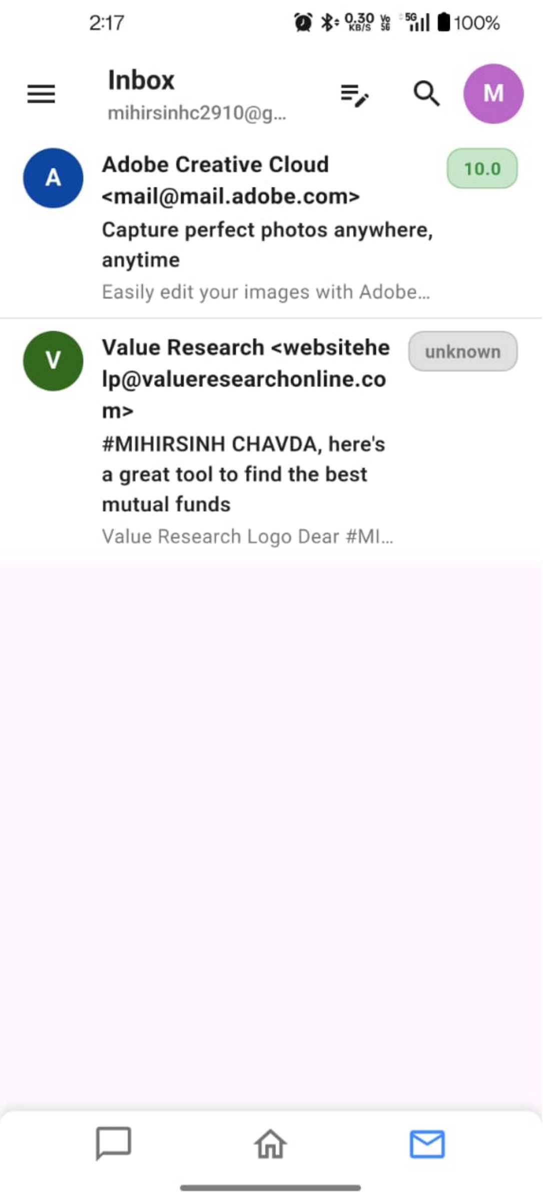
- Use strong, unique passwords and rotate them periodically.
- Verify the domain of a website



Suryadeepsinh Gohil <gohils...

Request to borrow some money.

Dear Mihir, I hope you are doing w...



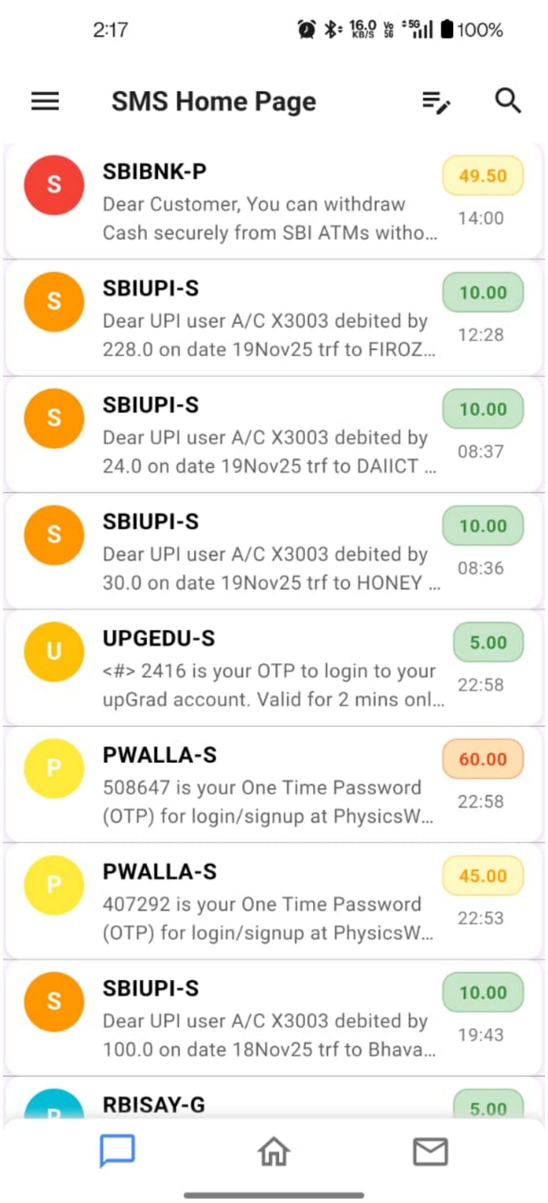
2:17 100%

Inbox
mihirsinhc2910@g...

Adobe Creative Cloud <mail@mail.adobe.com>
Capture perfect photos anywhere, anytime
Easily edit your images with Adobe...
10.0

Value Research <websitehelp@valueresearchonline.com>
#MIHIRSINH CHAVDA, here's a great tool to find the best mutual funds
Value Research Logo Dear #MI...
unknown

SMS Integration and Permissions



SMS Home Page

S SBIBNK-P 49.50
Dear Customer, You can withdraw Cash securely from SBI ATMs witho...
14:00

S SBIUPI-S 10.00
Dear UPI user A/C X3003 debited by 228.0 on date 19Nov25 trf to FIROZ...
12:28

S SBIUPI-S 10.00
Dear UPI user A/C X3003 debited by 24.0 on date 19Nov25 trf to DAIICT ...
08:37

S SBIUPI-S 10.00
Dear UPI user A/C X3003 debited by 30.0 on date 19Nov25 trf to HONEY ...
08:36

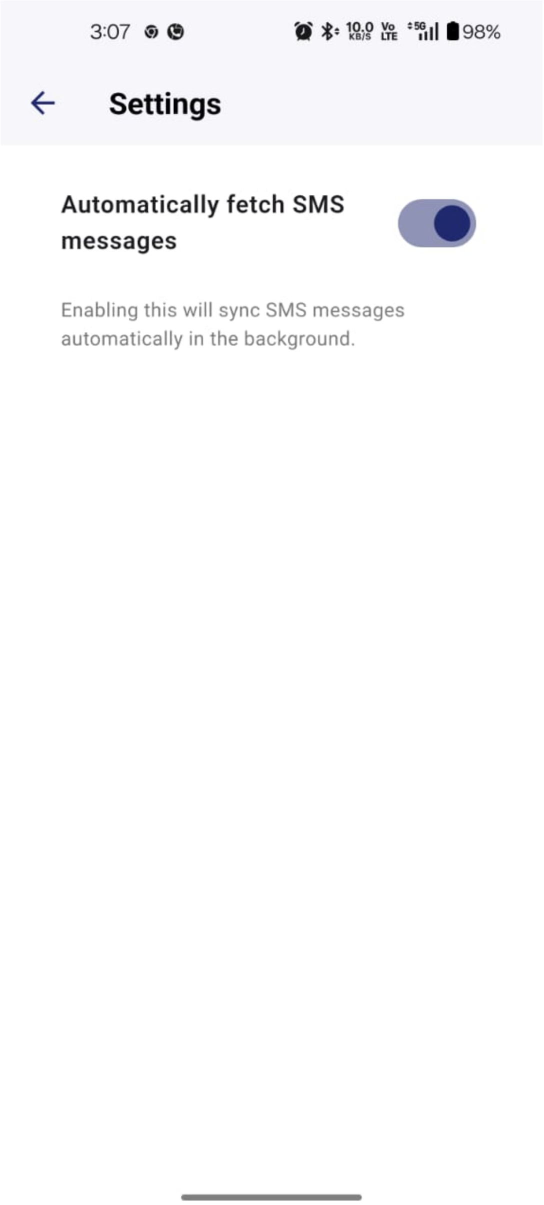
U UPGEDU-S 5.00
<#> 2416 is your OTP to login to your upGrad account. Valid for 2 mins onl...
22:58

P PWALLA-S 60.00
508647 is your One Time Password (OTP) for login/signup at PhysicsW...
22:58

P PWALLA-S 45.00
407292 is your One Time Password (OTP) for login/signup at PhysicsW...
22:53

S SBIUPI-S 10.00
Dear UPI user A/C X3003 debited by 100.0 on date 18Nov25 trf to Bhava...
19:43

RBISAY-G 5.00

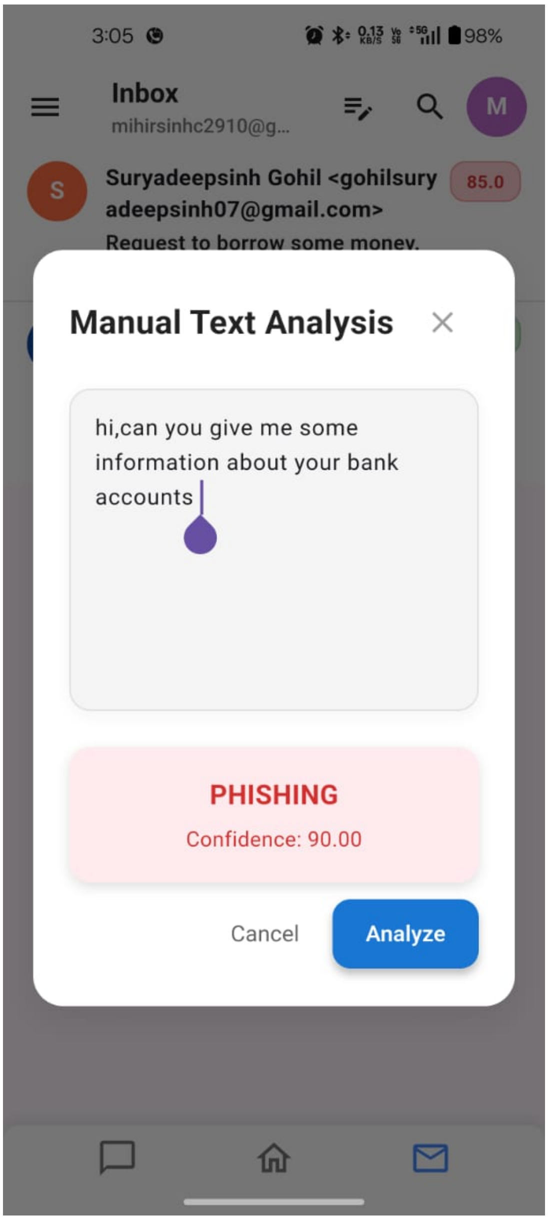


Settings

Automatically fetch SMS messages

Enabling this will sync SMS messages automatically in the background.

Advanced Detection and Manual Analysis



Suryadeepsinh Gohil <gohilsuryadeepsinh07@gmail.com>

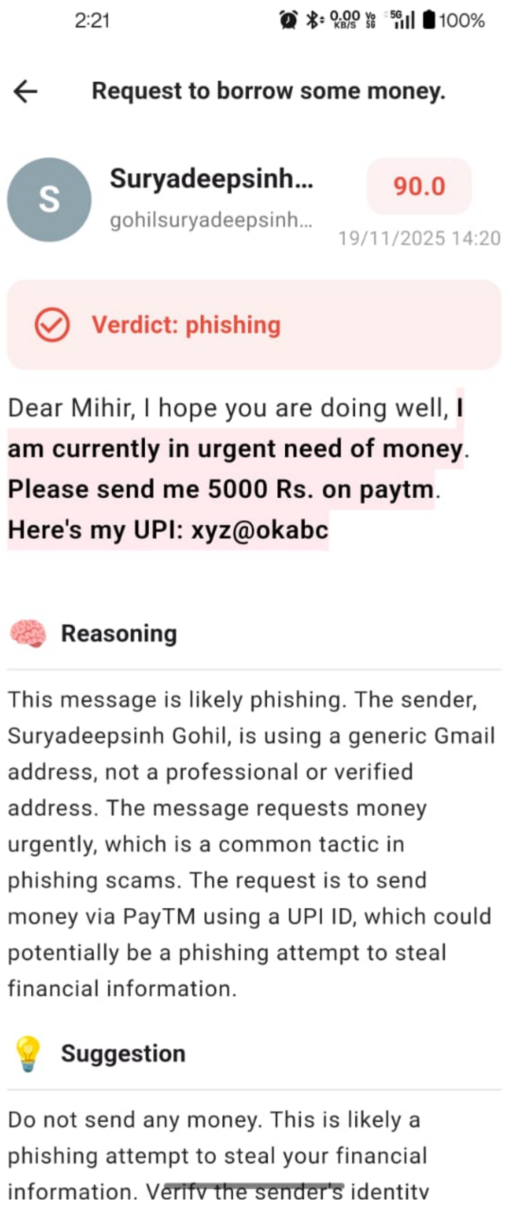
Request to borrow some money.

Manual Text Analysis

hi,can you give me some information about your bank accounts

PHISHING

Confidence: 90.00



Request to borrow some money.

Suryadeepsinh...

gohilsuryadeepsinh...

19/11/2025 14:20

Verdict: phishing

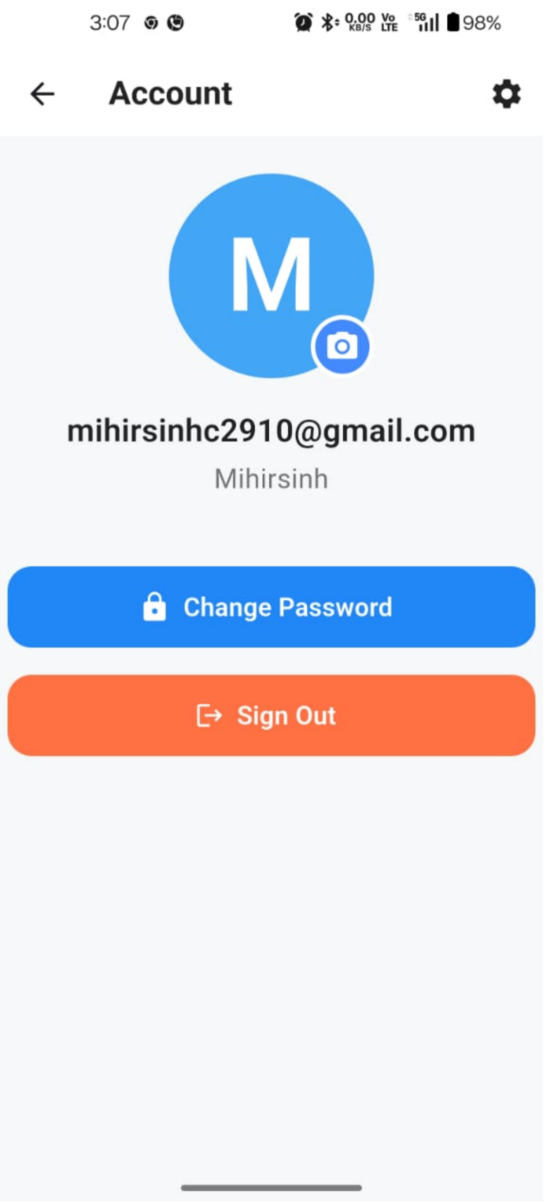
Dear Mihir, I hope you are doing well, **I am currently in urgent need of money**. **Please send me 5000 Rs. on paytm**. **Here's my UPI: xyz@okabc**

🧠 Reasoning

This message is likely phishing. The sender, Suryadeepsinh Gohil, is using a generic Gmail address, not a professional or verified address. The message requests money urgently, which is a common tactic in phishing scams. The request is to send money via PayTM using a UPI ID, which could potentially be a phishing attempt to steal financial information.

💡 Suggestion

Do not send any money. This is likely a phishing attempt to steal your financial information. Verify the sender's identity



mihirsinhc2910@gmail.com

Mihirsinh

Sprint 4 Report

Sprint Objective: Harden the application by implementing performance and security NFRs, and deliver personalization features where feasible.
Duration (Planned): 11 November – 17 November
Time Spent (Actual): 11 November – 19 November

Summary: Sprint 4 prioritized performance optimization and security hardening. Performance targets were met; several personalization items remained partially implemented.

Sprint Backlog (Sprint 4)

Epic-6 : Performance

US-16: Performance

Front Card

Target manual scan latency under 10 seconds and acceptable auto-scan response.

Epic-8 : Personalization

US-7 / FR-007: Push Notifications

Front Card

Deliver push notifications for high-risk detections.

Back Card

Status: Not implemented in the final build due to compatibility constraints.

US-9 / FR-009: Settings & Account

Front Card

Provide settings and account preferences.

Back Card

Status: Partially implemented. "Automatically Fetch SMS" toggle implemented and persisted.

Epic-9 : Security & Privacy

US-13: Privacy (Anonymous)

Front Card

Ensure message privacy by default; avoid storing raw content.

Back Card

Success:

- Only analysis metadata retained by default.

US-14: Secure Connections

Front Card

Enforce TLS for all API interactions and secure credentials.

Testing Strategy & Execution

Testing activities included:

- Unit testing and system testing.
- GUI testing and white-box testing.
- Mutation testing for model robustness.
- Non-functional testing for performance and security.

Sprint 4 — Review

- Performance: Manual scans meet the 10-second target; auto-scan pipeline is asynchronous and non-blocking.
- Personalization: Settings partially implemented; push notifications not included in final release.
- Security: TLS enforced and passwords stored using secure hashing; raw messages are not stored by default.
- De-scoped / Not implemented items are documented in the requirements-not-implemented appendix.

Project Conclusion

This project brings together all the work from Sprint 1 to Sprint 4 into a complete and usable system. The final build includes a reliable scanning pipeline, support for manual input, email and SMS scanning where allowed, background processing, and clear dashboards for users to view results and history. The multilingual analysis feature is implemented in its basic form and works for the intended use.

All features that were planned and built function as expected, and the system is stable for real use. The items listed in the appendix represent features that were considered earlier but were not included in the final build.

Appendix: Requirements Not Implemented

- Push notifications (FR-007) — not implemented due to notification/telephony compatibility issues on some Android versions.
- Full settings and language selection (FR-009) — partially implemented.
- Multilingual UI (FR-012) — not implemented in final build.
- User feedback loop (FR-006) — not implemented in final build.