

AegisSecure: AI-Powered Threat Detection App

Sprint 4 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 20, 2025



Formerly DA-IICT

IT314 - Software Engineering

Prof: Saurabh Tiwari

Mentor: Shyam Patel

Contents

Sprint Overview	3
Sprint Backlog	3
Testing Strategy & Execution	6
Sprint Review	6
Conclusion	7

Sprint Overview

Sprint Objective: To harden the application by implementing critical Non-Functional Requirements (NFRs) for performance (Epic 6) and security (Epic 9), and to deliver final personalization features (Epic 8).

Duration (Planned): 11 November – 17 November

Time Spent (Actual): 11 November – 19 November

A short summary: During Sprint 4, the team's final sprint, the focus was on hardening the application by implementing core performance targets (Epic 6) and critical security requirements (Epic 9). Some planned personalization items were only partially implemented — the Settings screen includes only the SMS auto-fetch toggle, and push notifications were not implemented. To finalize the project with a stable release, Epic 7 (User Feedback), US-7 (Push Notifications), and US-12 (Multilingual App UI) remained unimplemented, with Multilingual Analysis delivered only as a Beta version.

Sprint Backlog

Below are the Epics and User Stories planned and executed for this final sprint.

Note: The following features were either partially implemented or not implemented in the final submission (see Requirements Not Implemented / Challenges document).

- FR-006 / Epic 7 (User Feedback): **Not Implemented.**
- FR-007 / US-7 (Push Notifications): **Not Implemented.**
- FR-009 / US-9 (Settings & Account Preferences): **Partially Implemented.**
- FR-010 (Multilingual Analysis): **Partially Implemented (Beta).**
- FR-012 / US-12 (Multilingual App UI): **Not Implemented.**

Epic-6 : Performance

US-16: Performance

Front Card

As a user, I want fast scan results, so that I can act quickly.

Back Card

Success:

- Manual scan within 10s.
- Auto scan within 30s.

Failure:

- Delays longer than expected.
- App freezes during scan.

Epic-8 : Personalization

US-7 / FR-007: Push Notifications

Front Card

As a user, I want push notifications for threats, so that I can act accordingly.

Back Card

Status: Not Implemented.

Reason: Real-time push alerts were blocked by compatibility/configuration conflicts between the Telephony API and Android's notification requirements; integration could not be completed within the sprint timeline. **Planned Success Criteria:**

- Results shown in notification with numeric confidence and color-coded severity.

Failure / Current Behaviour:

- No push notification delivery in released build.
- Attempts to enable notifications may produce configuration errors on some Android versions.

US-9 / FR-009: Settings & Account

Front Card

As a user, I want account and preference settings, so that I can control how the app behaves.

Back Card

Status: Partially Implemented.

Implemented:

- "Automatically Fetch SMS" toggle implemented and persisted per user.

Not Implemented / Pending:

- Language selection in Settings.
- Notification controls (enable/disable notification categories).
- Full account preference management (profile edits, advanced toggles).

Failure / Current Behaviour:

- Other settings beyond SMS auto-fetch are unavailable in the current build.
- Notification controls are non-functional because push notifications are not implemented.

Epic-9 : Security & Privacy

US-13: Privacy (Anonymous)

Front Card

As a user, I want my message content to remain private, so that my sensitive data is not stored unnecessarily.

Back Card

Success:

- Only analysis output stored.
- No raw message saved.

Failure:

- Full message stored.

US-14: Secure Connections (Cyber Attack Proof)

Front Card

As a user, I want secure encrypted connections, so that my credentials and data remain safe.

Back Card

Success:

- HTTPS + encrypted API calls.
- Passwords encrypted.

Failure:

- Plain-text data transmission.
- Password stored in plain text.

Testing Strategy & Execution

In compliance with the course submission guidelines, the following testing strategies were implemented during Sprint 4 to ensure system stability, security, and performance:

- Unit Testing
- System Testing
- GUI Testing
- White Box Testing
- Mutation Testing
- Non-Functional Testing

Sprint Review

Overall, Sprint 4 was successful in hardening the application and delivering a polished, secure, and performant final product.

Performance & Model Accuracy (Epic 6)

We successfully optimized the scan pipeline. The system now effectively employs a multi-modal pipeline combining Statistical ML, Deep Learning, and LLMs. Experimental results indicate that the Ensemble model achieves **99.2% accuracy**, significantly outperforming isolated models. Manual scans are returning within the 10-second target, and the asynchronous processing flow ensures non-blocking analysis for auto-scans.

Personalization (Epic 8)

Push notifications (US-7 / FR-007) were **not implemented** due to Telephony API / Android notification compatibility issues. The team could not complete a stable notification flow within the sprint timeline.

The Settings screen (US-9 / FR-009) is **partially implemented**: the "Automatically Fetch SMS" toggle works and persists user preference. Other planned preferences (language selection, notification controls, and extended account management) remain pending.

Security & Privacy (Epic 9)

The final security NFRs were met. All connections are enforced over HTTPS (US-14), and passwords are encrypted. Crucially, user privacy is respected as the app does not store raw message content (US-13); only analysis metadata is retained.

De-scoped / Not Implemented Work

To ensure a timely and stable final release, several items remained unimplemented or only partially implemented:

- FR-006 / Epic 7 (User Feedback) — **Not Implemented**.
- FR-007 / US-7 (Push Notifications) — **Not Implemented**.
- FR-009 / US-9 (Settings & Account) — **Partially Implemented** (SMS auto-fetch only).
- FR-010 (Multilingual Analysis) — **Partially Implemented (Beta)**.
- FR-012 / US-12 (Multilingual App UI) — **Not Implemented**.

Team Progress

This final sprint solidified our skills in end-to-end development. The team successfully integrated complex model architectures (including BERT, Bi-LSTM, and Llama 4) into a cohesive backend structure while maintaining modularity. We successfully delivered a complete, secure, and performant application, concluding the project's development cycle.

Conclusion

Sprint 4 concludes the development of AegisSecure with important NFR hardening completed for performance and security. The integration of the Forensic Judge (Llama 4) and the hybrid ensemble model has resulted in a highly accurate detection system. However, several planned personalization features were only partially delivered: push notifications were not implemented (FR-007), the settings page is partially implemented (FR-009), and the user feedback loop was not implemented (FR-006). Despite these exclusions, the final build meets the core performance, accuracy, and security objectives targeted for this sprint.