- **Software Requirements Specification (SRS) – G-Mail Login Page**

Table of Contents

Project Name: Gmail Login Page

Prepared By: Yashri Sawant

Date: 08-10-2025

1. Introduction

i. Purpose

The purpose of this document is to provide a detailed description of the Gmail application developed by Google. It outlines the functional and non-functional requirements, system features, and interface specifications. The primary goal of Gmail is to provide users with a reliable, fast, and secure email communication platform accessible through web and mobile interfaces.

ii. Document Conventions

- Requirements are numbered for easy reference (e.g., FR-1, NFR-1).
- Bold text indicates section titles.
- Italics are used for emphasis.
- “Shall” indicates a mandatory requirement.

iii. Intended Audience and Reading Suggestions

This document is intended for:

- Developers: To understand system functionalities and implement features.
- Testers: To design and perform verification and validation tests.
- Project Managers: To track progress and ensure all requirements are met.
- End Users: To understand application capabilities.

iv. Project Scope

Gmail is a cloud-based email service allowing users to send, receive, and organize emails efficiently. It provides storage, spam filtering, multi-device synchronization, contact management, and integration with other Google services like Drive, Meet, and Calendar. The system supports both web and mobile platforms.

v. References

- IEEE Std 830-1998: IEEE Recommended Practice for Software Requirements Specifications
- Google Gmail Help Documentation
- Google API Documentation for Gmail

2. Overall Description

i. Product Perspective

Gmail is part of the Google Workspace ecosystem and interacts with various components such as Google Contacts, Google Drive, and Google Calendar. It relies on client-server architecture, where the client (web/mobile) communicates with the Gmail backend via secure APIs over HTTPS.

ii. Product Features

- Email sending, receiving, and organization
- Spam and phishing filtering
- Labels and folders for email categorization
- Advanced search functionality
- Integration with Drive, Meet, and Calendar
- Offline email access
- Multi-language support
- Real-time chat and video conferencing

iii. User Classes and Characteristics

- Regular Users: Individuals using Gmail for personal communication.
- Business Users: Users utilizing Gmail through Google Workspace.
- Administrators: Manage user accounts, permissions, and security policies.
- Developers: Integrate Gmail using APIs for custom applications.

iv. Operating Environment

- Web Browsers: Chrome, Firefox, Edge, Safari
- Mobile Devices: Android and iOS platforms

- Servers: Hosted on Google Cloud infrastructure
- Protocols: HTTPS, IMAP, POP3, SMTP

v. Design and Implementation Constraints

- Must comply with Google's Material Design guidelines.
- End-to-end encryption and OAuth 2.0 authentication.
- Support for high concurrency and minimal downtime.
- Cross-browser compatibility.
- Scalable cloud-based architecture.

vi. User Documentation

The Gmail system shall include user-oriented documentation to ensure smooth onboarding and usability.

i. User Manual

- A detailed guide describing Gmail's primary features, including sending, receiving, organizing, and searching emails.
- Step-by-step procedures for setting up an account, configuring settings, and integrating with Google services.
- Troubleshooting section covering common issues (e.g., login problems, spam settings, email delivery delays).
- Visual illustrations for common workflows such as composing mail, using labels, or setting up filters.

ii. Online Help and Tutorials

- Integrated help center accessible from the Gmail interface ("?" icon).
- FAQs addressing account recovery, spam control, privacy, and storage management.
- Interactive tutorials and video guides for first-time users.

iii. Developer Documentation

- API reference documentation for developers integrating Gmail services into third-party apps.
- Guidelines for using Gmail REST APIs, OAuth 2.0 authentication, and quota management.

- Sample code snippets in multiple programming languages (Python, JavaScript, Java).

iv. Release Notes

- Each new release will include documentation outlining new features, bug fixes, deprecated functionalities, and known issues.

vii. Assumptions and Dependencies

- Users must have an internet connection.
- Google account required for login.
- Relies on Google Cloud and associated APIs.
- Compatible with latest versions of browsers and OS.

3. External Interface Requirements

i. User Interfaces

- Web Interface: Clean, responsive layout using Material Design.
- Mobile Interface: Native applications for Android and iOS with push notifications.
- Accessibility: Support for screen readers, high contrast mode, and keyboard shortcuts.

ii. Hardware Interfaces

- Requires internet-enabled devices (PC, laptop, smartphone).
- Mobile devices require a functioning camera and microphone for Meet integration.

iii. Software Interfaces

Integration with:

- Google Drive (for attachments)
- Google Calendar (for scheduling)
- Google Meet (for video calls)
- Google Contacts (for address book)

iv. Communications Interfaces

- Secure communication using HTTPS and TLS.
- Email transfer via SMTP, IMAP, and POP3.
- OAuth 2.0 for authentication.

- JSON and REST APIs for third-party integrations.

4. System Features

i. Functional Requirements

ID	Requirement Description
FR-1	The system shall allow users to register and log in using a Google account.
FR-2	The system shall allow users to compose, send, receive, and delete emails.
FR-3	The system shall automatically categorize emails into Primary, Social, and Promotions tabs.
FR-4	The system shall provide spam detection and move spam messages automatically.
FR-5	The system shall allow users to attach files up to 25 MB and integrate with Drive for larger attachments.
FR-6	The system shall provide search functionality using keywords, sender, or date.
FR-7	The system shall support multi-device synchronization.
FR-8	The system shall allow users to archive, label, or star important emails.
FR-9	The system shall support email forwarding and filtering rules.
FR-10	The system shall notify users in real-time for new emails.

5. Nonfunctional Requirements

i. Performance Requirements

- The system shall handle at least 10 million concurrent users.
- Email delivery latency shall be under 2 seconds for intra-Google emails.
- System uptime shall be 99.9%.

ii. Safety Requirements

- Data backup and recovery mechanisms in case of system failure.
- Safe logout to prevent session hijacking.
- Automatic logout after prolonged inactivity.

iii. Security Requirements

- Two-factor authentication (2FA) for user accounts.
- End-to-end encryption of email data.
- OAuth 2.0 authorization framework.
- Regular security audits and vulnerability patching.

iv. Software Quality Attributes

- Reliability: Continuous uptime and auto-recovery.
- Usability: Simple and intuitive interface with tutorials.
- Scalability: Supports growing user base and new features.
- Maintainability: Modular code design for easy updates.
- Portability: Works seamlessly on web and mobile platforms.

v. Business Rules

Business rules define constraints, policies, and logical operations governing Gmail's behavior.

Rule ID	Business Rule Description
BR-1	Every Gmail user must have a unique Google account (email ID).
BR-2	Users must accept Google's Terms of Service and Privacy Policy before account activation.
BR-3	Emails larger than 25 MB shall be automatically uploaded to Google Drive with a shared link.
BR-4	Spam detection must be automatically applied to all incoming emails using machine learning algorithms.
BR-5	Deleted emails remain in the Trash folder for 30 days before permanent deletion.
BR-6	Users must authenticate via OAuth 2.0 when accessing Gmail from third-party applications.
BR-7	Gmail shall synchronize user data across all logged-in devices in real time.
BR-8	Two-Factor Authentication (2FA) must be enforced for high-risk login attempts.
BR-9	All emails shall be transmitted over secure channels (HTTPS/TLS).
BR-10	Account activity from new or suspicious devices must trigger security alerts.
BR-11	Gmail accounts inactive for more than 24 months shall be subject to deactivation or data removal per Google policy.
BR-12	User consent is required before Gmail integrates data from other Google Workspace apps.
BR-13	Attachments must be scanned for viruses and malware before download.
BR-14	Automatic logout shall occur after 30 minutes of inactivity for security purposes.
BR-15	Gmail shall not deliver identical promotional emails multiple times within 24 hours to the same user.

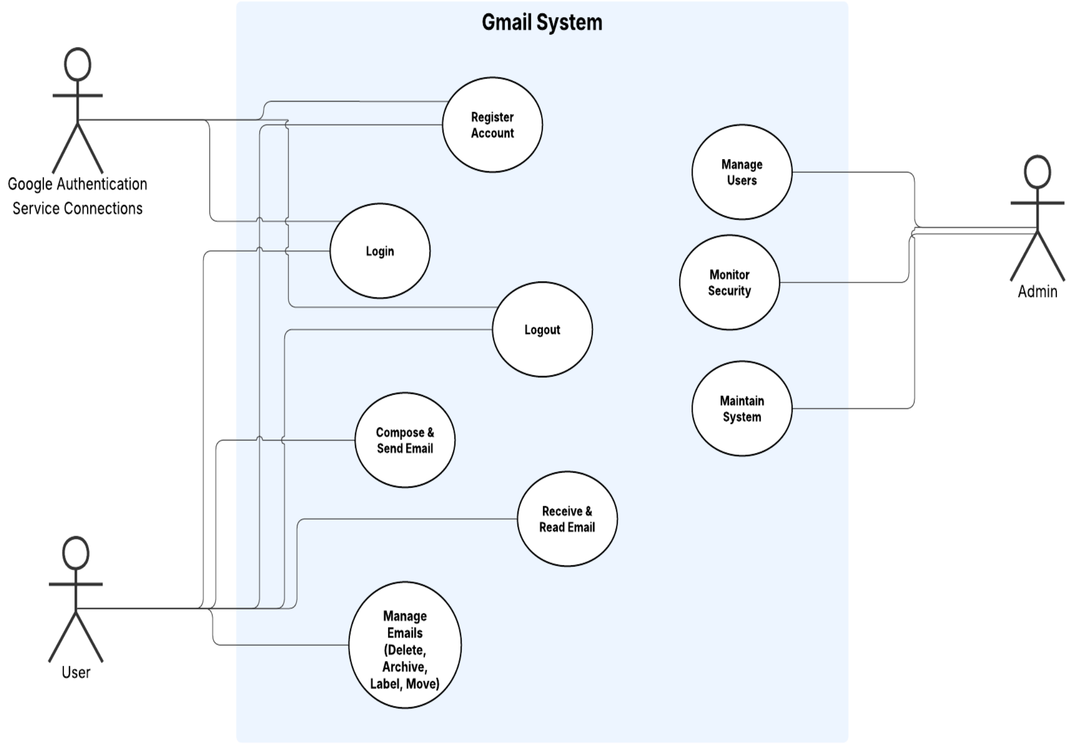
6. Other Requirements

i. Glossary

Term	Description
Gmail	A free email service developed by Google that allows users to send, receive, and manage emails.
Email Threading	Grouping of related messages with the same subject into a single conversation view.
Label	A tag assigned to emails for organization and filtering instead of folders.
Spam Filter	A mechanism that detects and isolates unwanted or suspicious emails.
Archive	A feature to remove emails from the inbox without deleting them.
Google Workspace	A collection of cloud-based productivity tools including Gmail, Drive, Meet, Docs, and Calendar.
End-to-End Encryption	Security mechanism ensuring only the sender and recipient can read the content of an email.

ii. Analysis Model

- **Use Case Diagram**



iii. To-Be-Determined (TBD) List

TBD ID	Description	Pending Decision
TBD-1	Exact maximum number of emails allowed per account.	Awaiting confirmation from Google backend team.
TBD-2	Frequency and method for data backup.	Decision pending on automated vs. manual backup policy.
TBD-3	Duration for OTP validity in 2FA.	Security team to finalize time threshold (e.g., 30 sec or 60 sec).
TBD-4	Integration timeline with future Google Workspace apps (e.g., Gemini AI).	Awaiting roadmap confirmation from product team.
TBD-5	Final accessibility compliance level (WCAG 2.1 AA or AAA).	Design and accessibility teams to decide.
TBD-6	Notification delivery mechanism for offline devices.	To be reviewed by mobile architecture team.
TBD-7	Exact SLA for global uptime under high concurrency.	Infrastructure team to define.
TBD-8	Limit on third-party API access rate.	To be confirmed by API management team.
TBD-9	Retention period for user analytics data.	Legal and compliance review required.
TBD-10	Default user storage quota for free Gmail accounts.	Awaiting policy update from Google Workspace team.