SOFTWARE REQUIREMENTS SPECIFICATION (SRS)

Rakshak – Android-Based Mobile Threat Awareness System

Team Name: RakshaTech

University: Centurion University of Technology and Management, BBSR

Domain: Cybersecurity (Mobile Security)

**1. Introduction**

**1.1 Purpose**

Rakshak is an Android-based security application designed to protect users from mobile threats such as spam calls, spam SMS, malicious files, unsafe app permissions, and cyber fraud. The purpose of this document is to describe the system requirements, features, and functional specifications of the Rakshak application.

**1.2 Scope**

Rakshak will:

* Detect spam calls and SMS
* Scan files and folders for malicious content
* Track and monitor app permissions
* Provide chatbot-based cyber assistance
* Perform phone health checkups
* Educate users about cyber threats

The system will improve digital safety awareness and enhance mobile security for Android users.

**2. Overall Description**

**2.1 Product Perspective**

Rakshak is a standalone Android application that integrates:

* Machine learning-based detection system
* Local file scanning engine
* Android permission monitoring APIs
* AI-powered chatbot
* Device health monitoring system

It interacts with:

* Call and SMS services
* Installed applications list
* Android OS
* User device storage

**3. System Features**

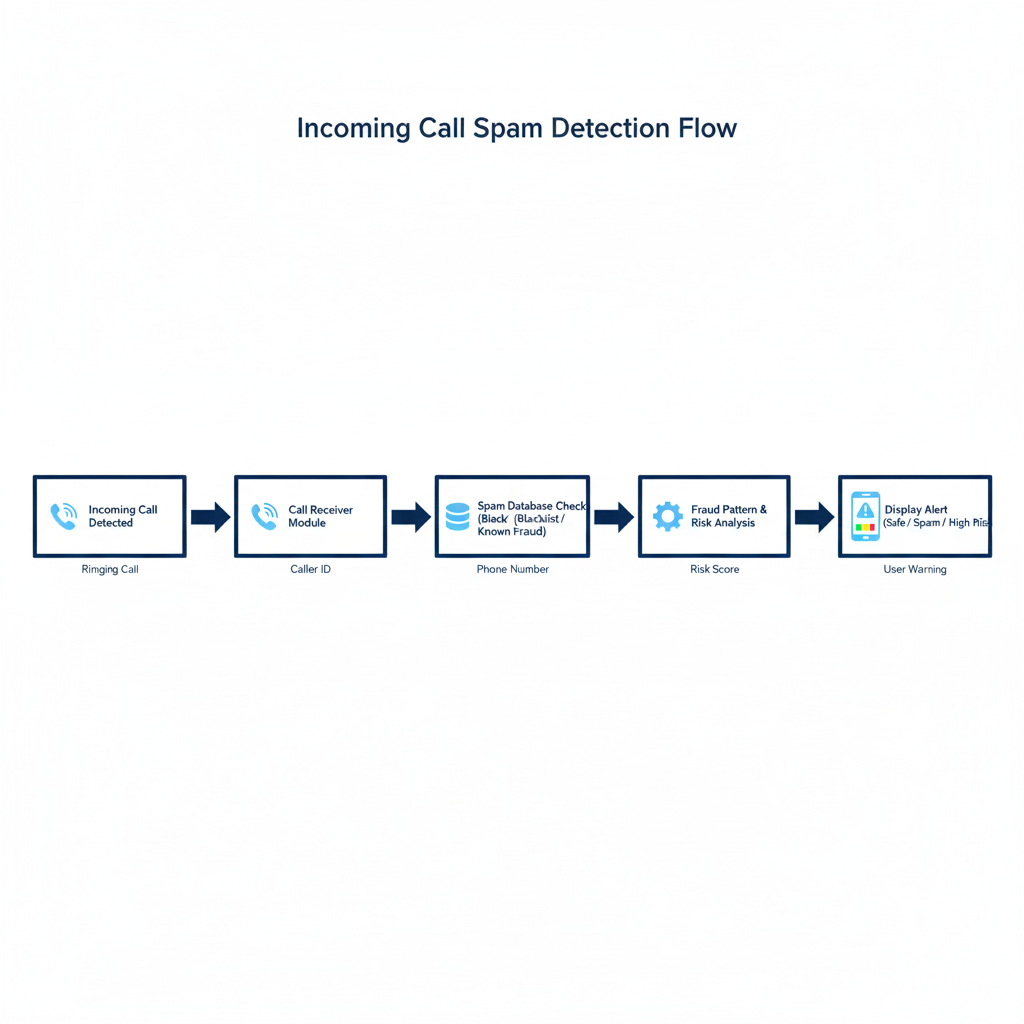
**3.1 Call Spam Detection System**

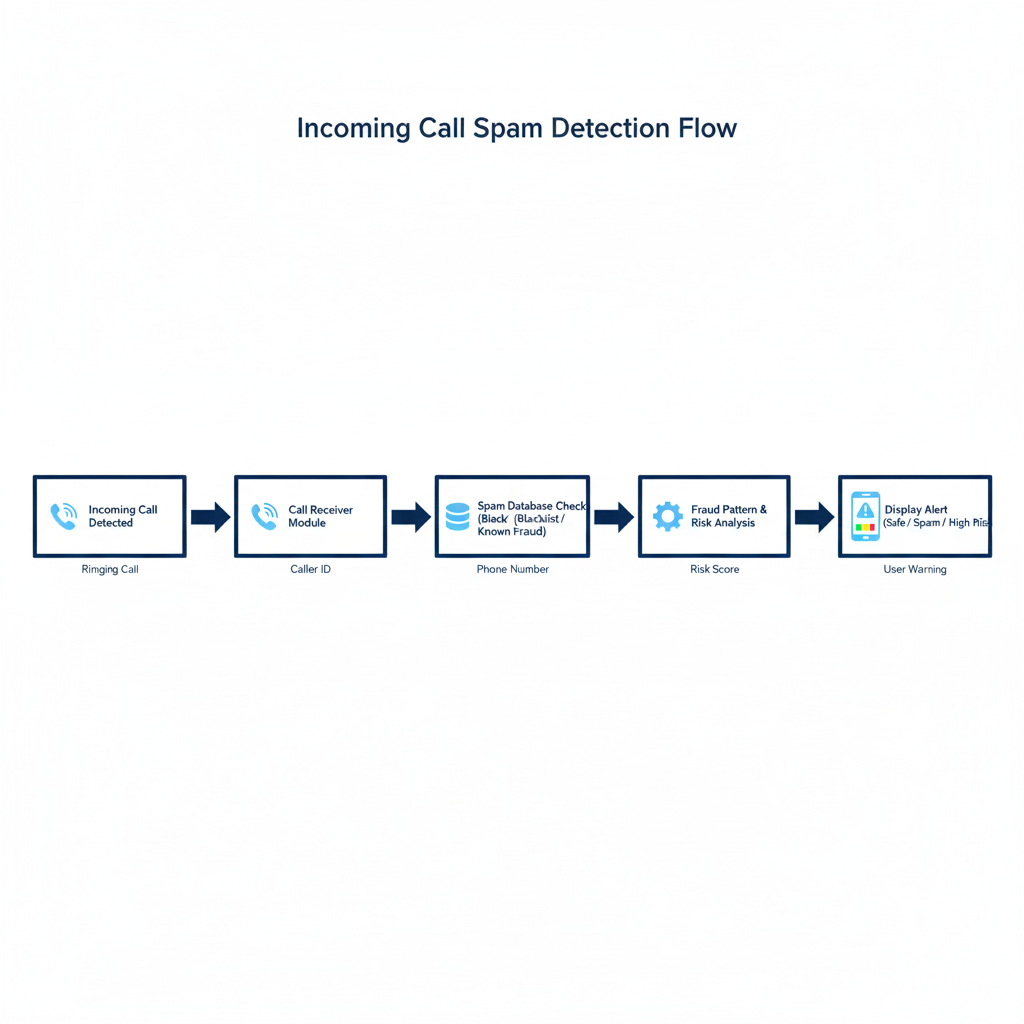
**📌 Description:**

Detects and blocks spam/fraud calls in real-time.

**🔹 Functional Requirements:**

* FR1: The system shall monitor incoming calls.
* FR2: The system shall analyze unknown numbers using spam database/ML model.
* FR3: The system shall notify the user if a call is suspected spam.
* FR4: The system shall allow users to block/report numbers.
* FR5: The system shall maintain a spam history log.

**🔹 Working:**



**3.2 SMS Spam Detection System**

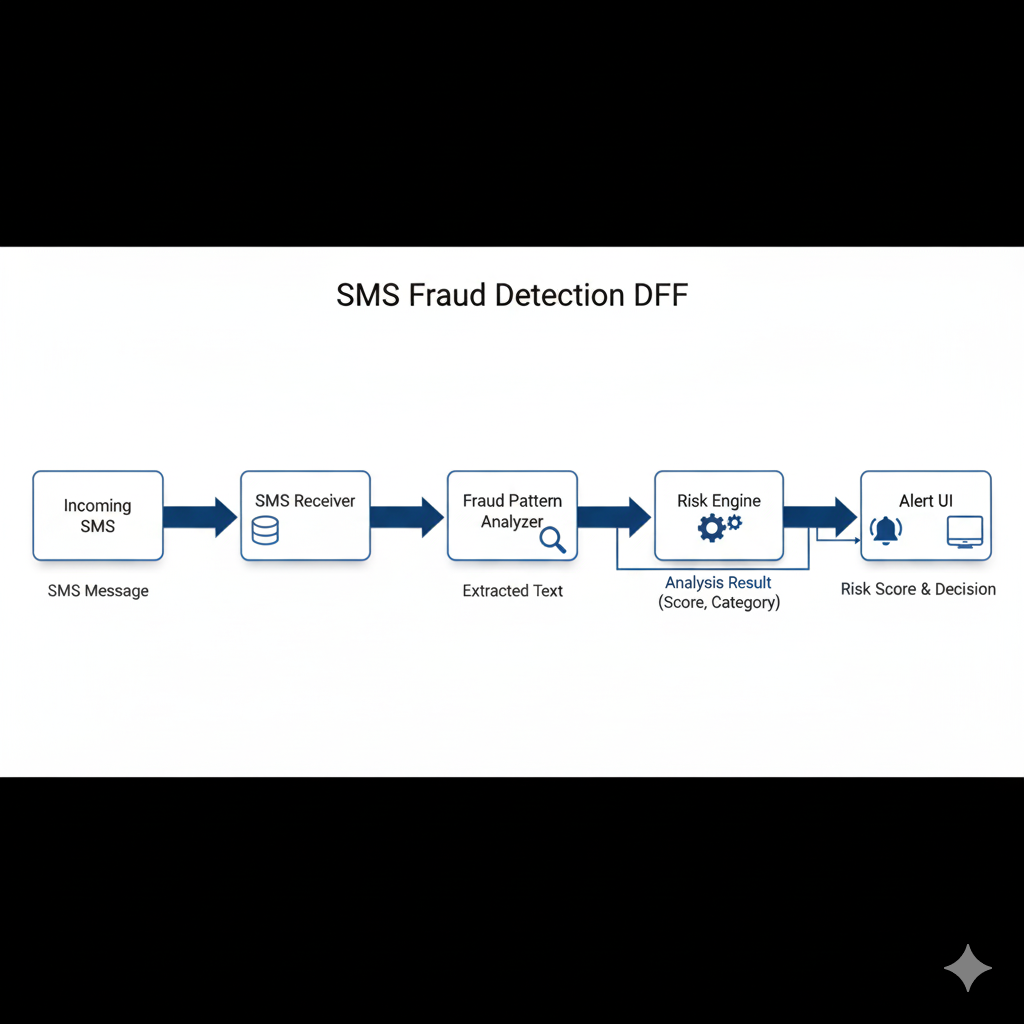
**📌 Description:**

Detects phishing, fraud, and spam messages.

**🔹 Functional Requirements:**

* FR1: The system shall scan incoming SMS.
* FR2: The system shall analyze message content using keyword/ML detection.
* FR3: The system shall categorize SMS as:
  + Safe
  + Promotional
  + Suspicious
  + Fraud
* FR4: The system shall alert the user if SMS contains malicious links.

**🔹 Woking:**



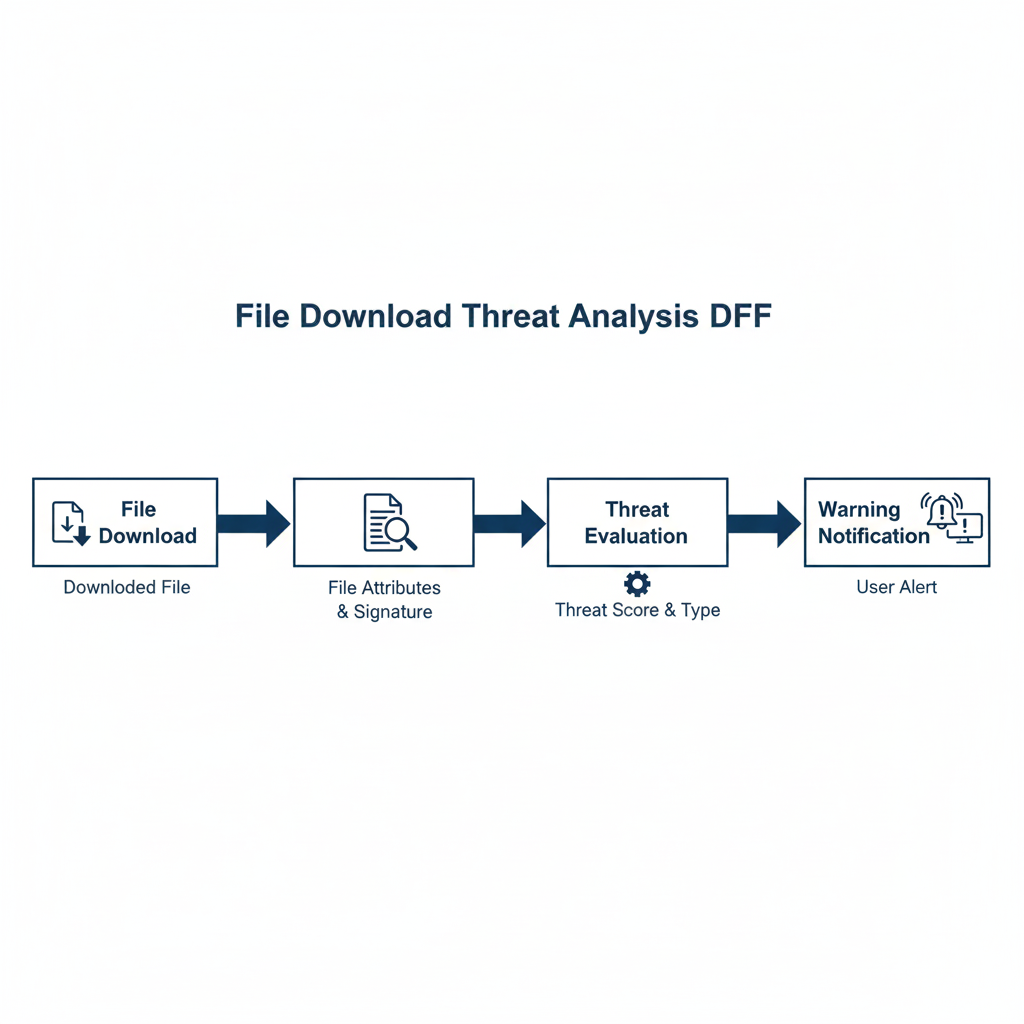
**3.3 File & Folder Scanner**

**📌 Description:**

Scans device storage to detect malicious files.

**🔹 Functional Requirements:**

* FR1: The system shall allow users to scan selected file/folder.
* FR2: The system shall detect:
  + Suspicious APK files
  + Hidden malware files
  + Corrupted files
* FR3: The system shall show scan results with threat level.
* FR4: The system shall allow file deletion.

**🔹 Working:**

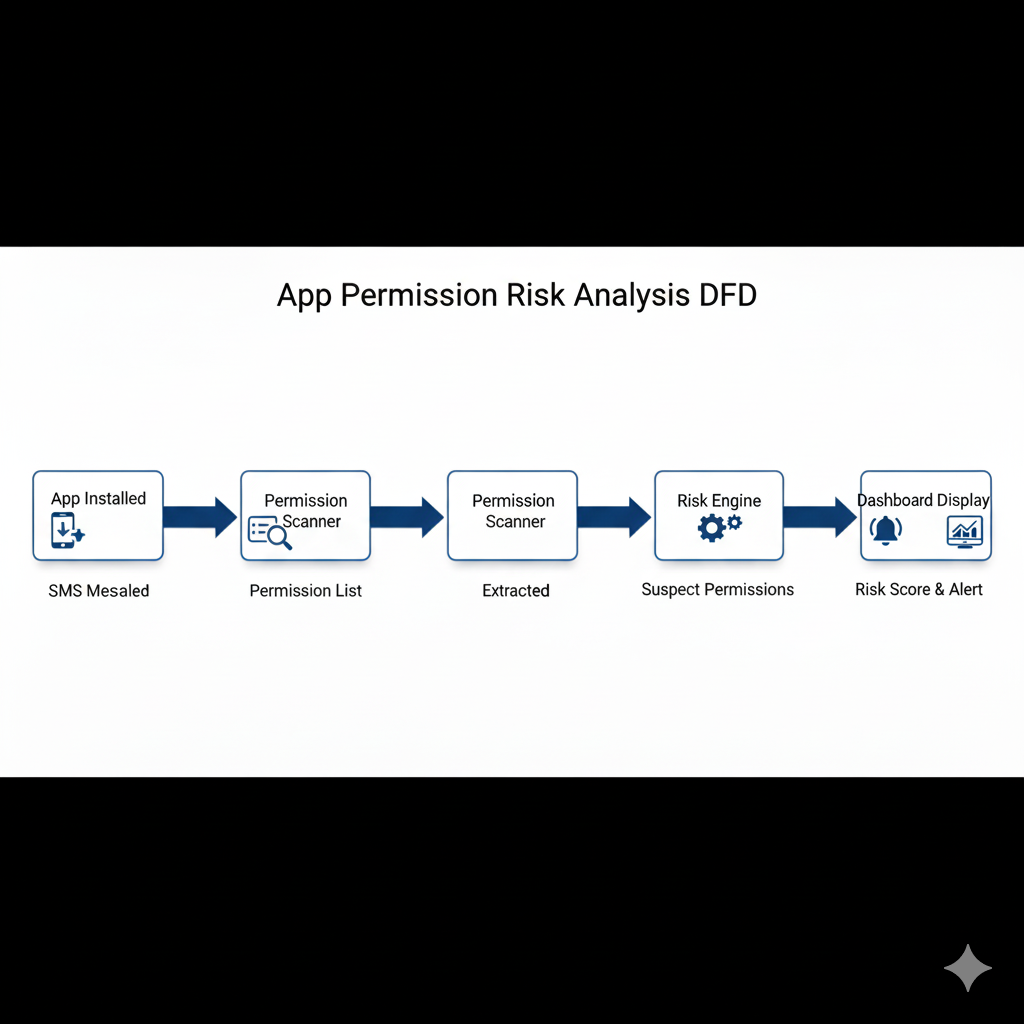
**3.4 Permission Tracker System**

**📌 Description:**

Tracks dangerous permissions used by installed apps.

**🔹 Functional Requirements:**

* FR1: The system shall list all installed applications.
* FR2: The system shall display permissions used by each app.
* FR3: The system shall highlight high-risk permissions like:
  + Camera
  + Microphone
  + Contacts
  + SMS
  + Location
* FR4: The system shall show permission usage frequency.
* FR5: The system shall guide users to revoke permissions.

**🔹 Working:**

**3.5 Chatbot Integration (Cyber Assistant)**

**📌 Description:**

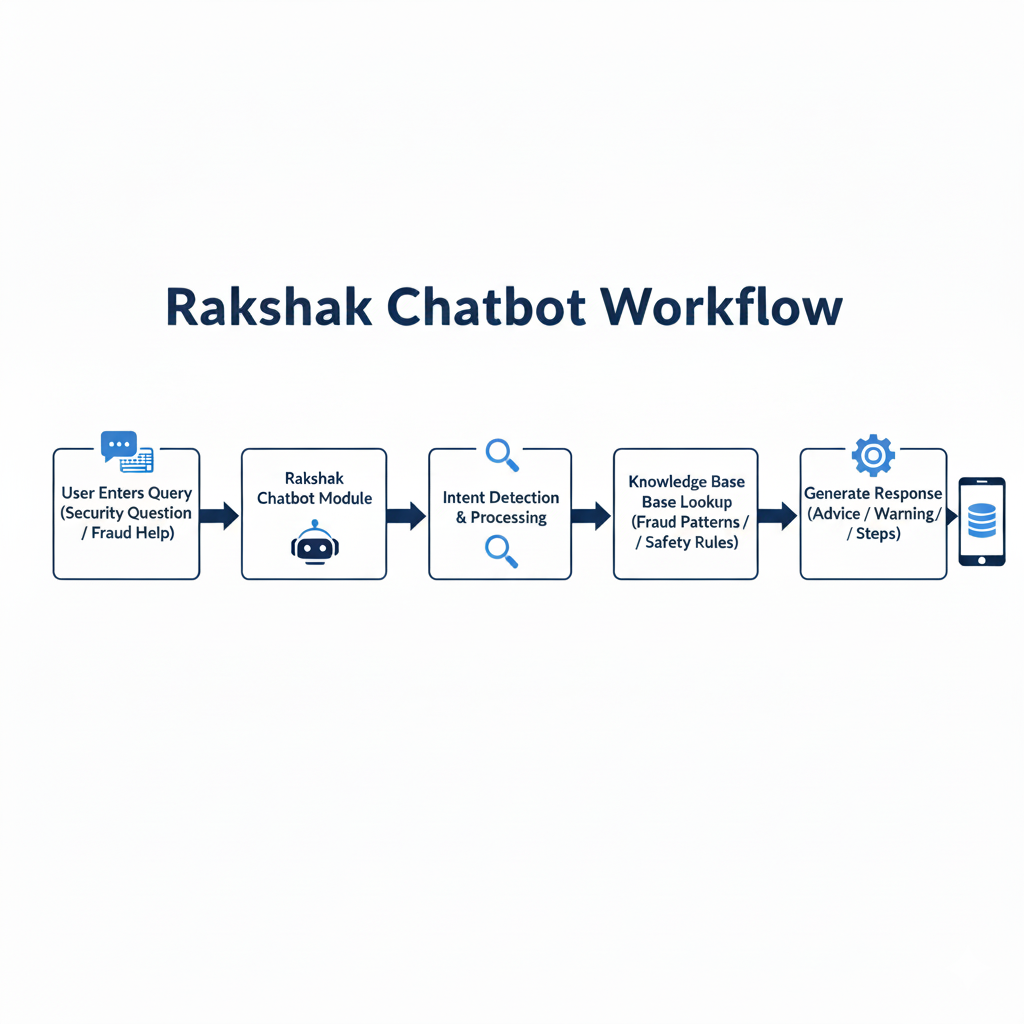
An AI chatbot that helps users in cyber fraud situations.

**🔹 Functional Requirements:**

* FR1: The chatbot shall answer cybersecurity-related questions.
* FR2: The chatbot shall provide fraud reporting steps.
* FR3: The chatbot shall guide users in case of scam.
* FR4: The chatbot shall provide awareness tips.
* FR5: The chatbot shall provide emergency helpline numbers.

**🔹 Example Queries:**

* “I received OTP scam message”
* “How to report cyber fraud?”
* “Is this link safe?”

**🔹 Working:**

**3.6 Phone Health Checkup System**

**📌 Description:**

Monitors device performance and security status.

**🔹 Functional Requirements:**

* FR1: The system shall show RAM usage.
* FR2: The system shall show storage usage.
* FR3: The system shall detect battery-draining apps.
* FR4: The system shall detect suspicious background activity.
* FR5: The system shall generate device health score.

**🔹 Health Metrics:**

* CPU usage
* RAM usage
* Storage usage
* Battery health
* Security score

4. Non-Functional Requirements

Performance: SMS detection must occur within 1 second.

Security: All fraud detection shall be processed locally.

Usability: Alerts must be clearly visible with warning symbols.

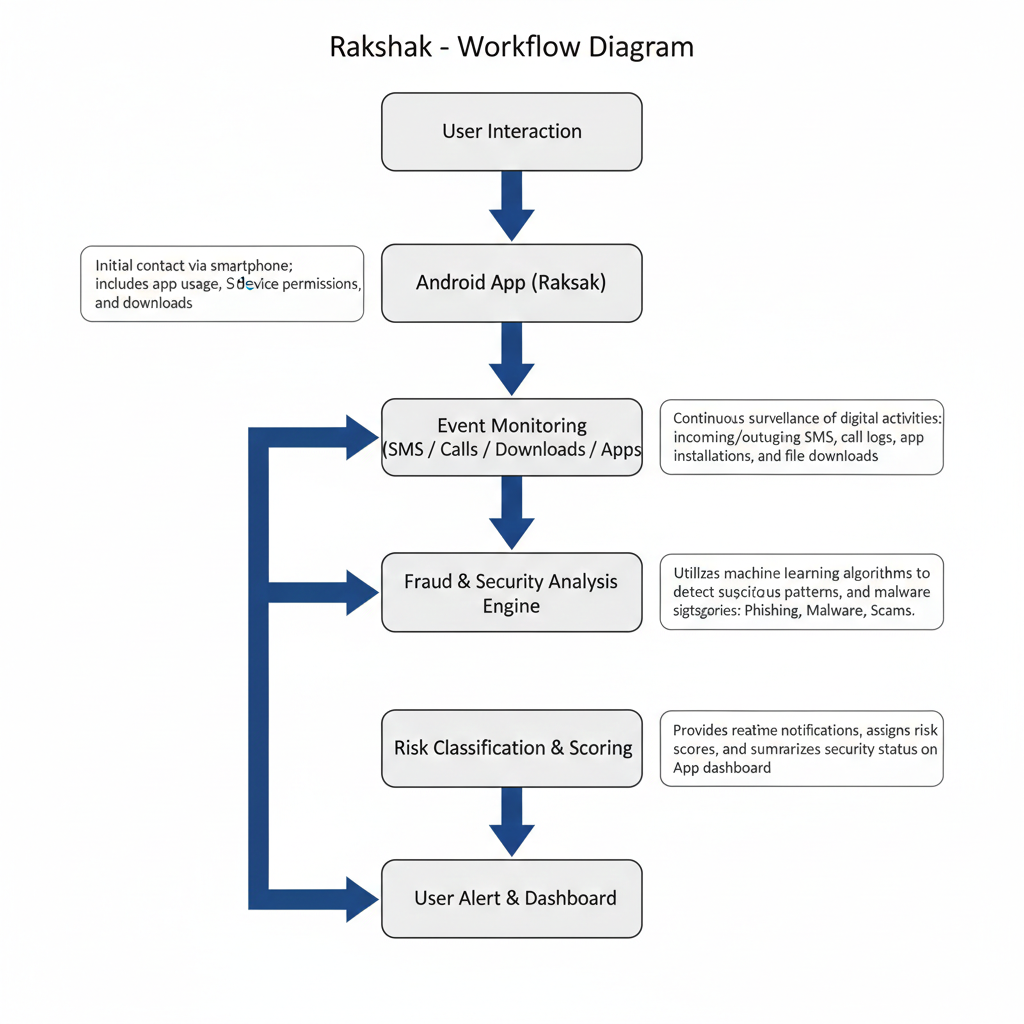
Reliability: System must not crash during background monitoring.

Maintainability: Modular architecture for easy updates.

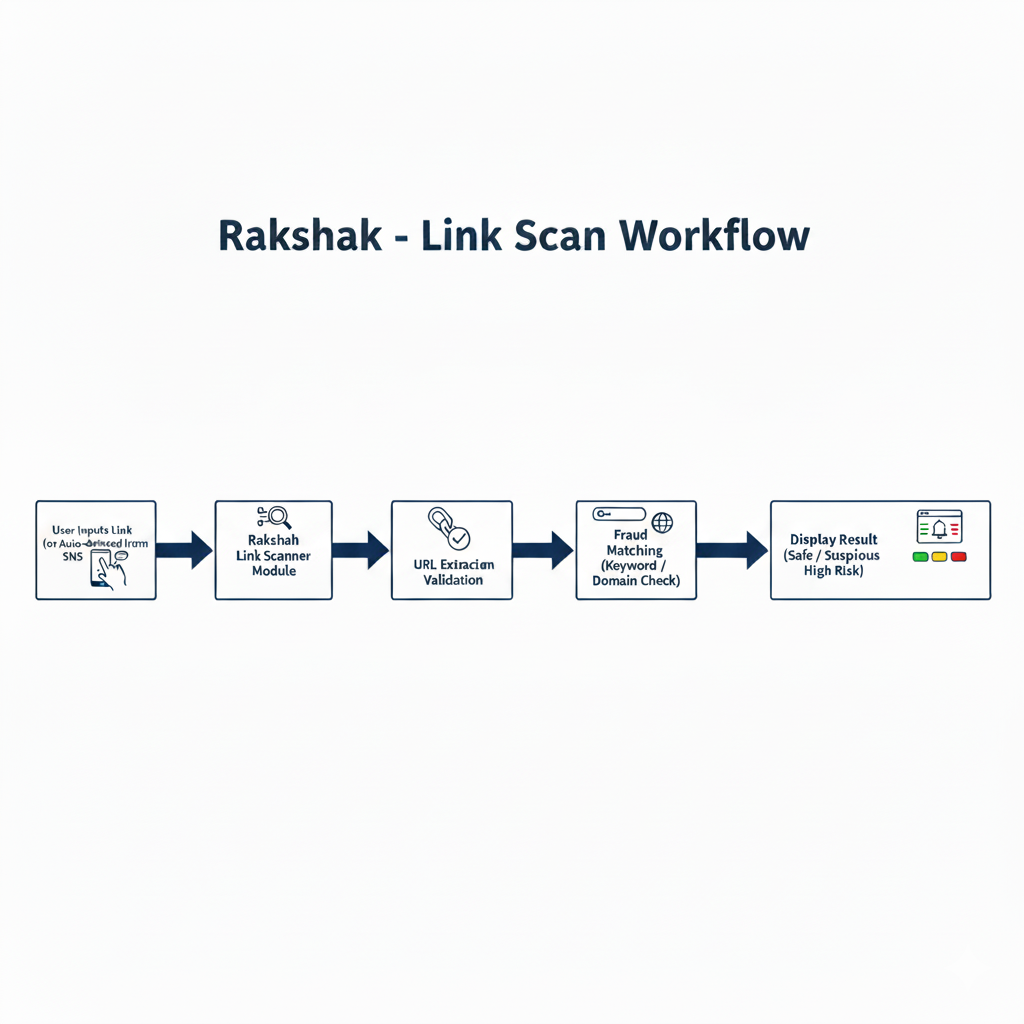
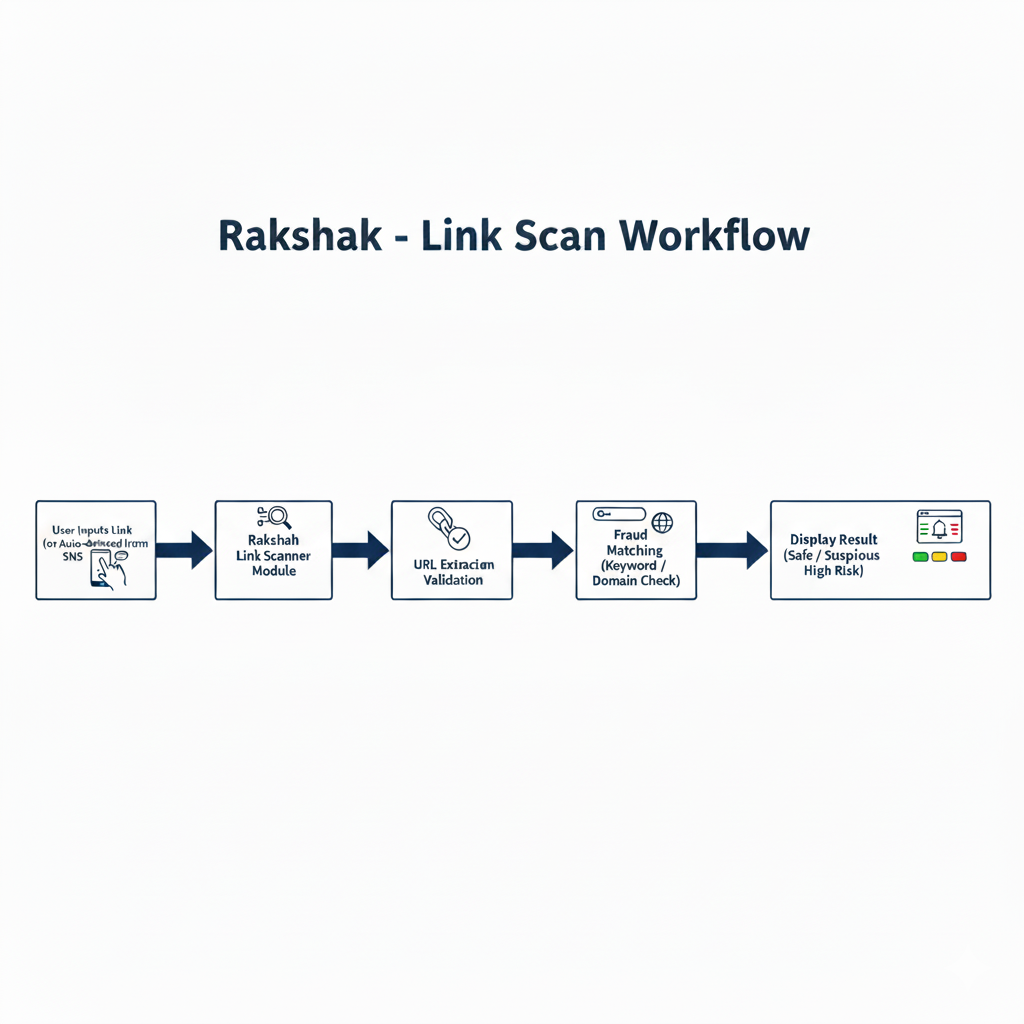
5. System Architecture

5.1 Overall System Architecture Diagram

User interacts with Rakshak System. The system processes incoming SMS, calls, and app data, analyzes threats, and provides alerts to the user.



5.2 Data Flow Diagram



6. Use Case Diagram Description

Primary Actor: User

Receive Fraud Alert

Scan Installed Apps

View Risk Dashboard

Scan Suspicious Link

Chat with Security Assistant

Activate Emergency Fraud Mode

The user interacts with the system to monitor threats and receive real-time warnings.

7. Innovation & Feasibility

Unified mobile threat awareness system.

Fraud-pattern based SMS detection for Indian scam scenarios.

Permission intelligence dashboard.

No root access required; fully compliant with Android policies.

8. Impact & Benefits

Reduces financial fraud risks.

Improves user security awareness.

Protects sensitive personal and financial data.

Scalable for future AI-based enhancements.

9. References

Android Developer Security Documentation

Android Permission and Sandbox Model

OWASP Mobile Top 10 Security Risks

Mobile phishing and scam analysis reports