Software Requirements Specification

AI spam detector : Shielding Against Cyber Threads

Harshadip Vijay Umbakar (76)

**Table Of Contents**

1. Introduction
   1. Purpose
   2. Scope
   3. Definitions, acronyms and abbreviation
   4. References
2. Overall description
   1. Product perspective
   2. Product functions
   3. User characteristics
   4. Constraints
   5. Assumptions and dependencies
   6. Apportioning of requirements
3. Specific requirements
   1. External interface requirements
      1. User interfaces
      2. Hardware interfaces
      3. Software interfaces
      4. Communications interfaces
   2. Functional requirements
      1. User Class 1
      2. User Class 2

3.2.1 User Class 3

* 1. Performance requirements
  2. Design constraints

# Introduction

This section provides a scope description and overview of everything included in this SRS document. It explains the purpose of the project, defines important terms, and lists relevant references.

# Purpose

The purpose of this document is to outline the software requirements for the development of a **Mobile Cybersecurity Software** application. This system is designed to protect mobile devices from various digital threats such as malware, phishing attacks, unauthorized access, and data breaches. It defines the functional and non-functional requirements, system behavior, user interfaces, and constraints to guide development and ensure the delivery of a secure, efficient, and user-friendly application.

The primary audience for this document includes software developers, project managers, quality assurance testers, and stakeholders such as corporate IT security teams and individual users.

# Scope

The Mobile Cybersecurity Software is a mobile application for **Android** and **iOS** devices, offering comprehensive protection features. It includes:

* Malware scanning and removal
* Real-time threat detection and alerts
* Secure VPN for safe internet browsing
* App permission monitoring to prevent privacy violations
* Anti-phishing protection for web and email links
* Data encryption for sensitive files and communications

The software is intended for both **individual users** and **corporate clients**. It will feature a clean, intuitive interface, customizable security settings, and cloud-based updates for the latest threat intelligence.

# Definitions, Acronyms, and Abbreviations

|  |  |
| --- | --- |
| **Term / Acronym** | **Definition** |
| **VPN** | **Virtual Private Network — encrypts internet traffic and hides user location** |

|  |  |
| --- | --- |
| **Term / Acronym** | **Definition** |
| **AES** | **Advanced Encryption Standard — secure encryption algorithm** |
| **UI** | **User Interface** |
| **API** | **Application Programming Interface** |
| **MFA** | **Multi-Factor Authentication** |
| **SRS** | **Software Requirements Specification** |

* 1. **References**

1. Google Play Security Guidelines — https://developer.android.com/google/play/requirements/security
2. Apple iOS Security Guidelines — https://developer.apple.com/security

# Overall Description

This section gives an overview of the Mobile Cybersecurity Software, its system context, main features, intended users, and other relevant aspects such as constraints, assumptions, and development phases.

# Product Perspective

The Mobile Cybersecurity Software is designed as a standalone **mobile application** with optional integration into enterprise **Mobile Device Management (MDM)** systems.

It operates on both **Android** and **iOS** platforms and functions independently, but can also communicate with cloud-based threat intelligence services for real-time updates.

The application will have the following core modules:

* **Threat Detection Module** – Scans device storage and installed applications for malware, spyware, or trojans.
* **Real-Time Protection Engine** – Monitors system activity to block suspicious behavior instantly.
* **VPN & Secure Browsing Module** – Encrypts internet traffic and masks IP addresses.
* **App Permission Monitor** – Tracks and alerts users about risky app permissions.
* **Phishing Protection Module** – Detects malicious websites and fake login pages.
* **Reporting & Alerts Module** – Generates security status reports and sends real-time notifications.

The system will integrate with:

* Cloud-based threat databases
* Device OS security APIs (Android Play Protect, iOS Security APIs)
* Optional enterprise MDM platforms for centralized security management

# Product Functions

Key functionalities of the Mobile Cybersecurity Software include:

* **Malware Scan & Removal** — Detect and remove harmful files and applications.
* **Real-Time Threat Detection** — Instant alerts when suspicious activity is detected.
* **Secure VPN Connection** — Protects online privacy and prevents tracking.
* **Permission-Based Alerts** — Warns users when apps request sensitive permissions.
* **Phishing Prevention** — Blocks dangerous websites and email links.
* **Data Encryption** — Secures personal files and communication channels.
* **Security Reports & Analytics** — Provides a summary of detected threats and actions taken.

# User Characteristics

The Mobile Cybersecurity Software targets three main user groups:

* **Individual Users** — Mobile phone owners who want personal data protection and privacy.
* **Corporate Employees** — Workers using company-issued devices requiring enterprise-level security.
* **IT Administrators** — Responsible for monitoring and securing multiple devices in an organization.

All users are expected to have basic smartphone usage skills. IT administrators will require additional technical knowledge for managing enterprise configurations.

# Constraints

* Requires internet connectivity for VPN and threat database updates.
* Certain advanced features depend on operating system permissions and capabilities.
* Performance may vary on older mobile devices with limited memory and processing power.
* VPN service may be restricted in regions with internet censorship laws.

# Assumptions and Dependencies

* Users will keep the application and threat definitions updated.
* External threat intelligence providers will maintain accurate and timely databases.
* The application assumes that mobile OS security APIs will remain accessible and functional.
* The system depends on stable cloud server availability for real-time protection features.

# Apportioning of Requirements Phase 1 – Core Protection

* Malware scanning and removal
* Phishing protection
* Real-time alerts

# Phase 2 – Privacy & Network Security

* VPN integration
* Secure browsing mode

# Phase 3 – App Monitoring

* App permission tracking
* Privacy risk analysis

# Phase 4 – Enterprise & Advanced Features

* MDM integration for centralized management
* Advanced analytics dashboard
* Cloud-based AI threat prediction

# Specific Requirements

This section describes all functional, performance, and design requirements of the Mobile Cybersecurity Software, including details of interfaces and user roles.

# External Interface Requirements

* + 1. **User Interfaces**

The application will have a **modern, intuitive mobile UI** compatible with Android and iOS platforms.

* + - * **Home Dashboard** — Displays overall device security status, recent threats detected, and quick action buttons.
      * **Scan Page** — Allows manual scans for malware and vulnerabilities.
      * **VPN Control Page** — Enables and configures secure VPN connections.
      * **Permissions Monitor** — Lists all installed apps and their requested permissions with risk ratings.
      * **Reports Page** — Shows a history of security incidents and resolutions, with options to export reports.

# UI Features:

* + - * Simple icons and color coding for security status (Green = Safe, Yellow = Warning, Red = Threat).
      * Touch-optimized navigation.
      * Dark and light theme options.
      * Accessibility compliance with WCAG 2.1 guidelines.

# Hardware Interfaces

* + - * **User Devices:** Any Android (version 8.0 or later) or iOS (version 14 or later) device with at least 2GB RAM and 100MB free storage.
      * **Optional:** Biometric authentication (fingerprint/face recognition) for secure app access.
      * **Enterprise Option:** Integration with Mobile Device Management (MDM) hardware if available.

# Software Interfaces

* + - * **OS APIs:**
        + Android Device Administrator & Play Protect APIs.
        + iOS Security & VPN APIs.

# External APIs:

* + - * + Threat intelligence feeds from reputable providers (e.g., VirusTotal API).
        + VPN service APIs.

# Database:

* + - * + Cloud-based storage for security logs and threat signatures.

# Communication Interfaces

* + - * **Protocol:** All communication between the app and servers will use HTTPS with TLS

1.3 encryption.

* + - * **Authentication:** Secure login using OAuth 2.0 or MFA (Multi-Factor Authentication).
      * **Push Notifications:** Real-time alerts for detected threats.

# Functional Requirements User Class 1 – Individual User

* **FR1.1 – User Login** — Secure authentication using username/password or biometric methods.
* **FR1.2 – Manual Device Scan** — Ability to initiate a full or quick scan of the device.
* **FR1.3 – Real-Time Protection** — Automatic detection and blocking of malicious activities.

# User Class 2 – Corporate Employee

* **FR2.1 – Enterprise Login** — Login using corporate credentials (SSO or MDM integration).
* **FR2.2 – VPN Access** — Encrypted network tunnel for secure business communication.
* **FR2.3 – Compliance Reports** — Ability to generate security compliance reports for IT review.

# User Class 3 – IT Administrator

* **FR3.1 – Centralized Device Monitoring** — View and manage security status of multiple company devices.
* **FR3.2 – Remote Actions** — Remotely initiate scans or lock devices in case of compromise.
* **FR3.3 – Policy Enforcement** — Enforce security rules such as mandatory VPN use or restricted app installations.

# Performance Requirements

* **PR1 – Scan Speed:** Full device scan must complete within 5 minutes on standard devices.
* **PR2 – VPN Connection Time:** VPN must connect within 3 seconds under normal network conditions.
* **PR3 – Battery Usage:** The app should not consume more than 5% battery in the background over 24 hours.
* **PR4 – Concurrent Users:** The cloud backend must support at least 10,000 simultaneous users without degradation.

# Design Constraints

* **DC1 – Mobile-First Design:** Must be optimized for mobile devices only (no desktop version required).
* **DC2 – Cross-Platform Compatibility:** Must run smoothly on both Android and iOS.

# DC3 – Technology Stack:

* + **Frontend:** Native Android (Kotlin) and iOS (Swift).
  + **Backend:** Node.js or Django with PostgreSQL/MongoDB.
* **DC4 – Third-Party Dependency:** Relies on external threat intelligence APIs and VPN providers.