**Protect + Talk = ProtecTalk**

Real-Time Scam Call Detection and Alerts App

This document outlines the product requirements for the **ProtectTalk** app, designed for real-time scam call detection and alerting, with the option for an intervention by a contact person.

### **Application Overview**

In recent years, there has been a significant increase in telephone scams, particularly targeting vulnerable populations such as the elderly and people with mental disabilities, who are often more susceptible to these types of fraud. Scammers use sophisticated techniques to deceive their victims, often posing as representatives of banks, government authorities, insurance companies, or other trusted organizations in an attempt to steal money or personal information. These calls often come from unknown numbers or numbers that appear to be legitimate, making it difficult to identify scams in advance.

Our app, **ProtecTalk**, offers an innovative and effective solution to this growing issue, providing an additional layer of protection for users. The app operates automatically in the background, monitoring and detecting suspicious calls from unknown or potentially fraudulent numbers. Analyzes and predicts the likelihood of a scam call. Once there is a high probability of a suspicious call ongoing, the app sends a real-time alert to the user or directly to a designated contact, ensuring that someone is always informed and able to take action.

This alert allows the recipient of the call to decide whether to answer or not. If the call is identified as suspicious, they can avoid the conversation without exposing themselves to fraud. The goal is to provide peace of mind, particularly for elderly individuals and those with mental disabilities, while ensuring their privacy and security. The app is designed to be simple and easy to use for all age groups and abilities, helping to protect against scams while maintaining a sense of safety and confidence.

### 

### 

### 

### 

### 

### 

### 

### 

### **Product Requirements**

### 1. Application Overview

### 1.1. The application is designed for smartphones.

### 1.2. The application will operate on most Android devices worldwide.

### 1.3. The application will support devices with Android operating systems (at least two major versions behind the latest version).

### 1.4. The application will be available for free download on the Google Play Store.

### 1.5. The application will support English, with plans to expand to additional languages in the future.

### 2. Core Functionality and Value Proposition

### 2.1. Real-time scam call monitoring and alerts while preserving user privacy.

### 2.2. AI-powered fraud detection leveraging proprietary scam number databases and speech pattern recognition.

### 2.2.1. The fraud detection model will operate locally on the user’s device to ensure privacy and minimize data sharing.

### 2.2.2. The model will continuously learn and improve offline through cloud-based updates. These updates will be periodically sent to the device to keep the model up to date with the latest scam patterns and phone numbers.

### 2.2.3. The scam number blacklist will be stored on a secure server, ensuring that the system can identify and block known scam numbers with a high degree of accuracy.

### 2.3. Advanced fraud prevention capabilities, including real-time alerts.

### 2.3.1. If the incoming call number is found in the scam number blacklist, the call will be blocked automatically, preventing potential scams from reaching the user.

### 2.3.2. If the application identifies a fraudulent pattern based on speech and behavior analysis (even if the number is not in the blacklist), it will alert both the Protectee and the Protector. This ensures that both parties are informed of potential fraud risks in real-time.

### 

### 2.4. Low resource consumption – designed to operate efficiently with minimal impact on device performance. The application will run seamlessly in the background with a minimal battery and CPU load.

### 2.5. Offline functionality – the application will be capable of detecting and preventing scams even without an internet connection. The locally stored AI model will continue to assess incoming calls and issue warnings.

### 2.6. Simple and accessible interface – designed for all age groups, with a focus on accessibility features to accommodate users with disabilities.

### 2.7. Strong security and privacy – All data will be encrypted for user protection. There will be no long-term storage of sensitive data like transcripts. Only necessary information will be stored, and all data handling will be done transparently, in accordance with the privacy policy.

2.8. User Participation in Model Improvement - Users will have the option to share transcripts of suspicious calls with the cloud-based learning system. By doing so, they can help the model improve its fraud detection capabilities. Shared transcripts will be anonymized to ensure user privacy. They will be used solely to enhance the accuracy of the AI model in identifying scam calls. The system will provide users with clear information on the data sharing process, including the option to opt-out at any time.

### 3. User Identification and Permissions

### 3.1. User identification will occur after app installation by manually entering their phone number, then receiving a randomly generated 5-digit verification code.

### 3.2. During initial registration:

### 3.2.1. The user will accept the terms of use and privacy policy.

### 3.2.2. The user will allow access to the phone, microphone, contacts, and location to enable scam detection functionality.

### 

### 4. User Roles and Relationships

### 4.1. Users will be categorized into two groups:

### 4.1.1. Regular Users (Protectees): Individuals who receive protection from scam calls.

### 4.1.2. Protectors: Contacts assigned to help protect users.

### 4.2. User Details: For each user, the system will store the following information:

### 4.2.1. User Type (Protector / Protectee) – This determines the user's role in the system.

### 4.2.2. User's Name – The full name of the user for identification purposes.

### 4.2.3. User's Phone Number – The phone number associated with the user’s account.

### 4.2.4. Linked Contact/User Details – The information of other linked contacts or users (for example, Protectors or Protectees).

### 4.3. User Roles and Permissions:

### 4.3.1. Users will choose whether to request or provide protection during post-registration setup:

### 4.3.2. If requesting protection, the user will enter their protector’s details.

### 4.3.3. If providing protection, the user will enter the protectee’s details.

### 4.3.4. The details include the name, phone number, and relationship type.

### 4.4. Linking Limitations:

### 4.4.1. Protectees can have up to two protectors whose phone numbers are linked to their account.

### 4.4.2. Protectors can have an unlimited number of protectees whose phone numbers are linked to their account.

### 5. Protection Confirmation and Contact Management

### 5.1. Protection requests follow a two-way approval process for added security.

### 5.2. Protection requests will be managed and displayed in a dedicated management screen.

### 5.3. Users can add or remove contacts through the app settings.

### 5.4. Protectees can have up to two assigned protectors, while protectors can be linked to an unlimited number of protectees.

5.5. Uninstallation Notification- If a Protectee uninstalls the application, a notification will be sent to the Protector’s phone, informing them of the Protectee's action. This ensures that Protectors are aware of any changes in their linked Protectees.

### 6. Automatic Background Operation

### 6.1. The application will run continuously in the background without requiring manual activation.

### 6.2. It will warn users of scam calls without needing to open the app manually.

### 

### 7. Fraud Call Prediction and Prevention

### 7.1. The AI model will use regularly updated scam phone databases to identify fraudulent calls.

### 7.2. The model will compare incoming call numbers against the database to assess risk.

### 7.3. If the user answers an unidentified call:

### 7.3.1. The AI model will transcribe and analyze the conversation in real time.

### 7.3.2. Fraud probability will be calculated based on speech and behavioral patterns.

### 7.3.3. A warning will be issued if the call is predicted to be a scam.

### 7.3.4. The assigned protector will be notified (if applicable).

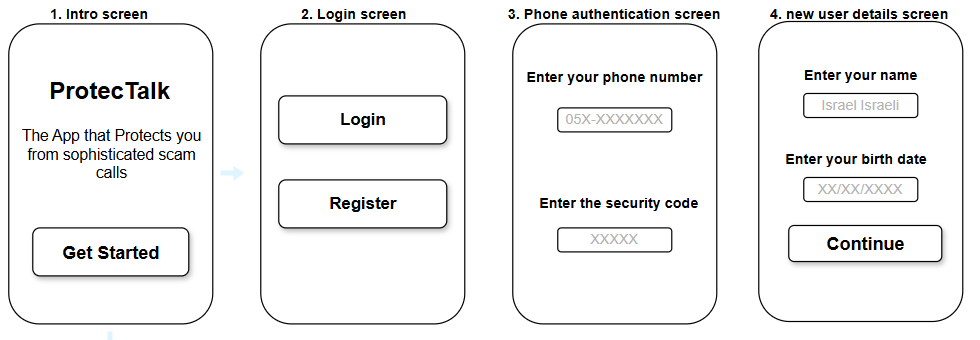
### 7.4. Optionally, the system can auto-block scam calls before they connect.

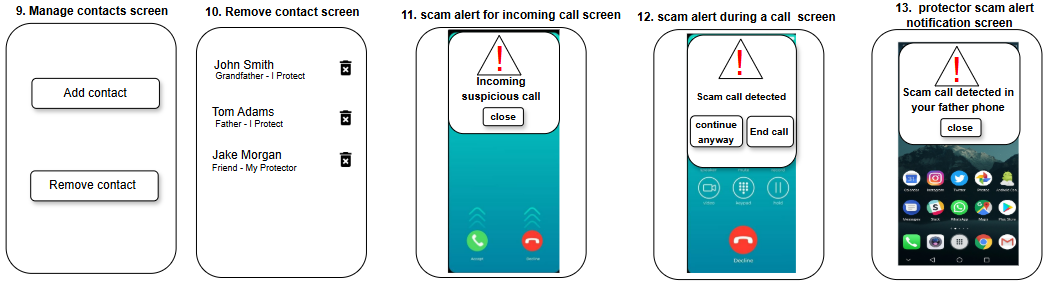
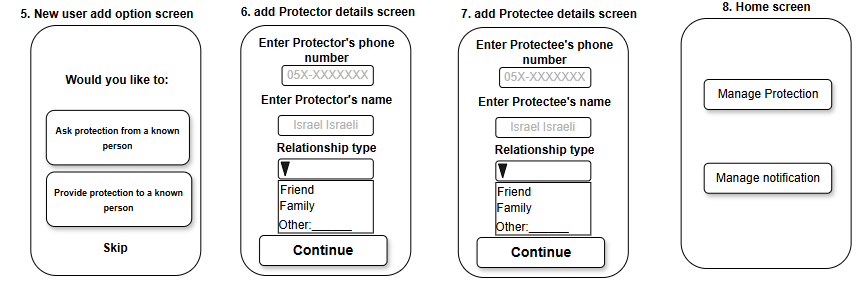
### 8. AI Learning and Continuous Improvement

### 8.1. The AI model continuously improves by learning from fraud patterns (without storing sensitive user data).

8.2 Scam phone databases are dynamically updated based on verified reports and call analysis.

### 

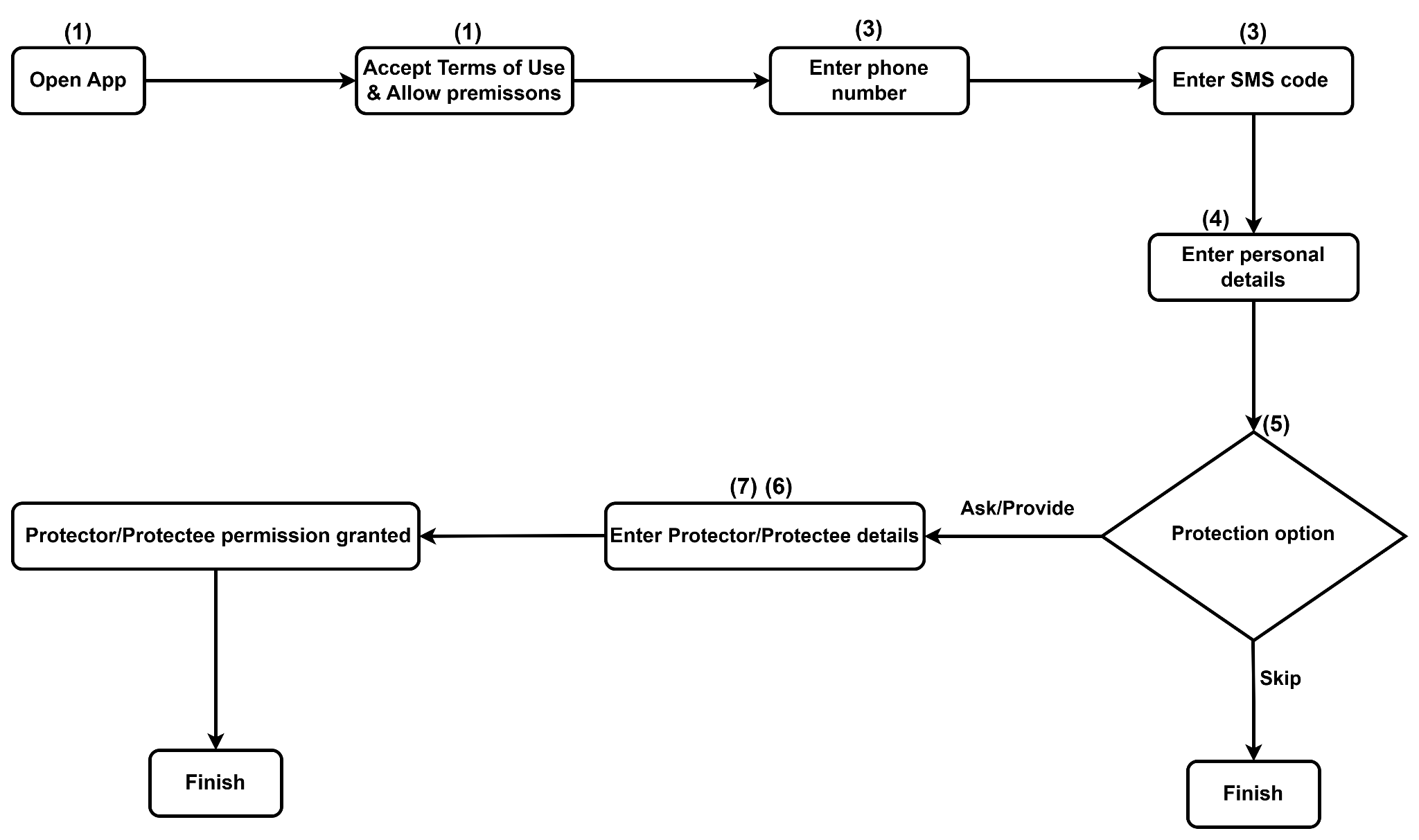
**Application screens**





**Application flowcharts**

### **1. Registration to the App**



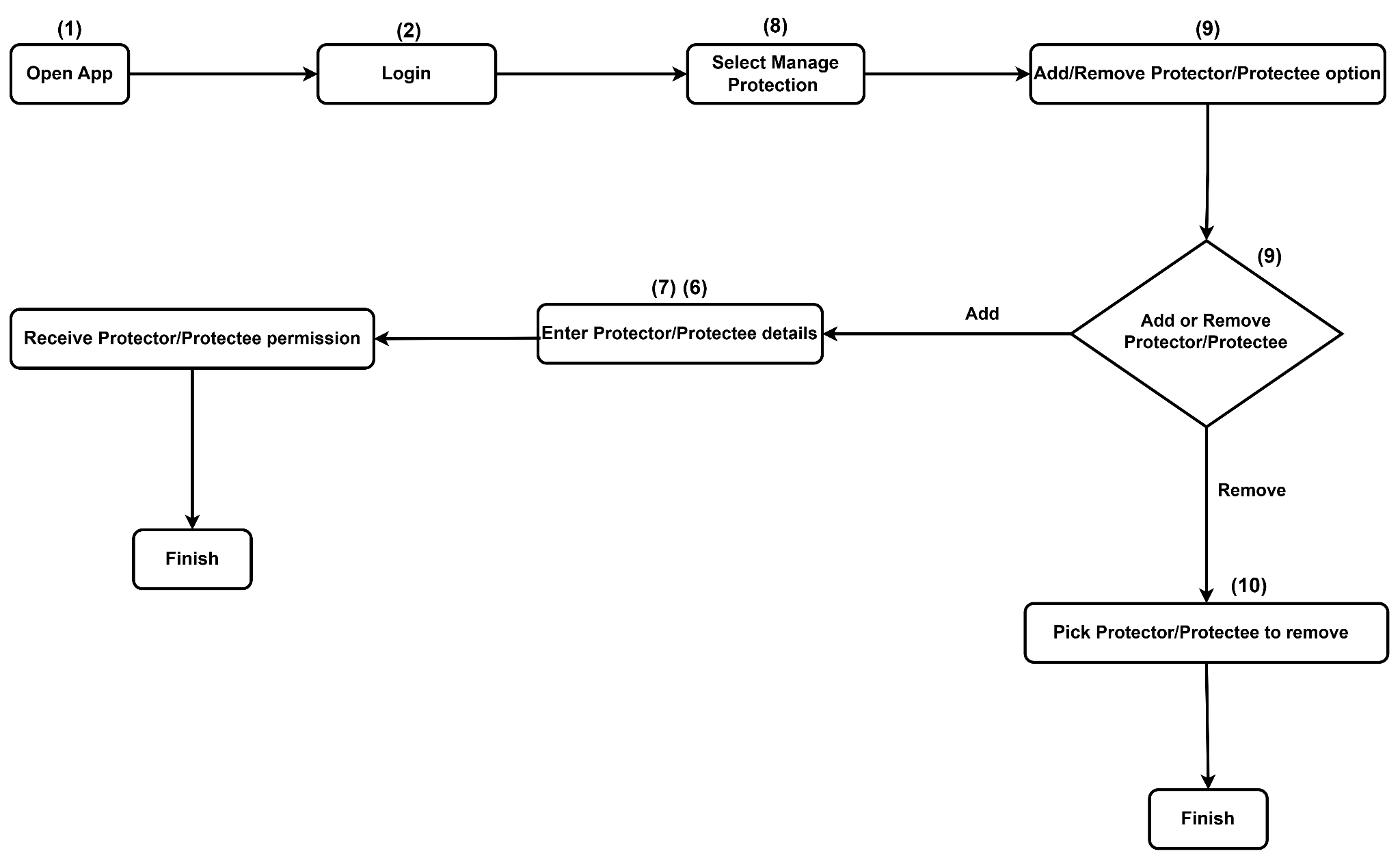
### 

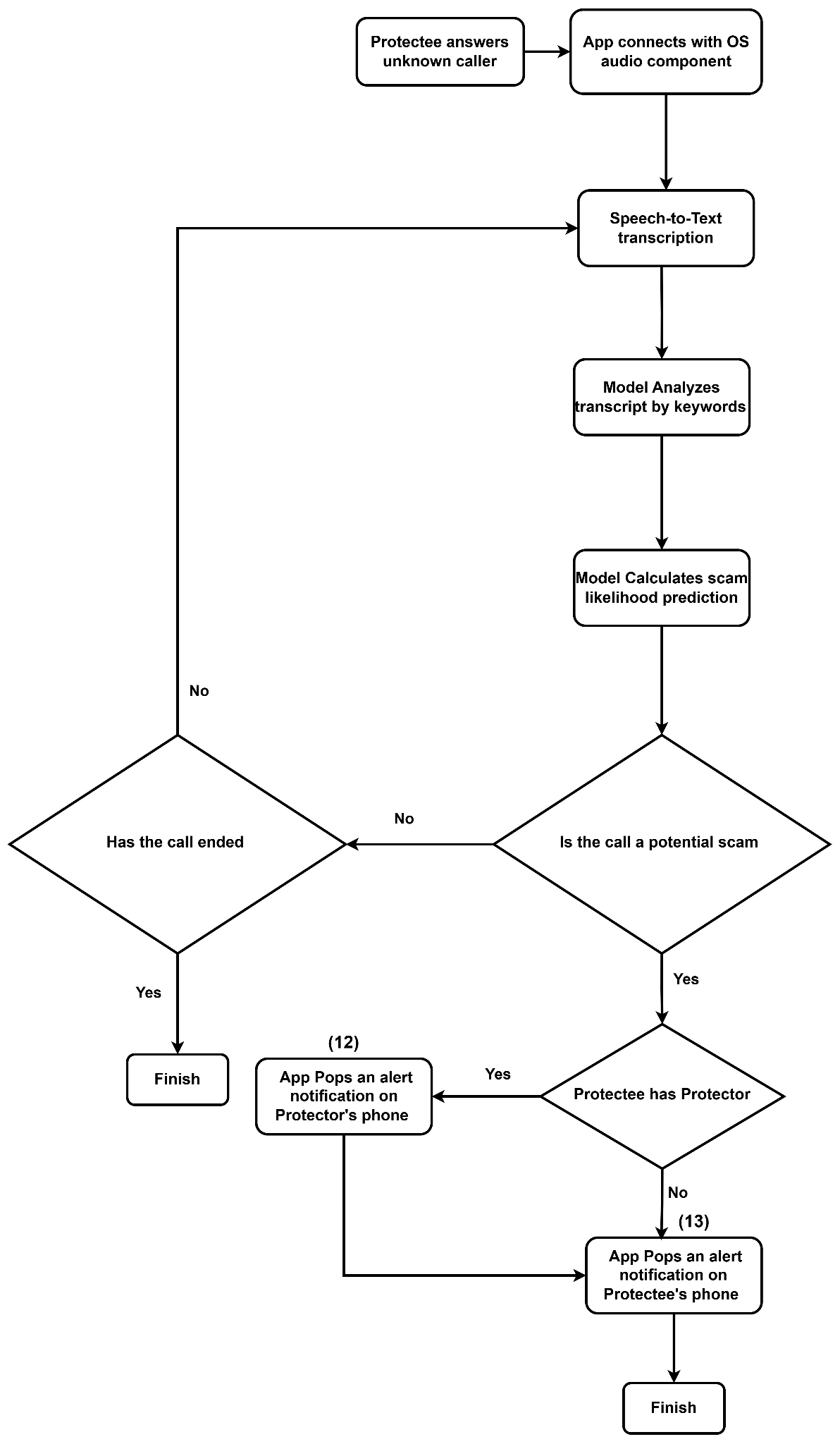
### 

### 

### 

### **2. Add/Remove Protector/Protectee**



**3. Real-time call notification using AI scam detection** 

### **4. Incoming suspicious call notification**

