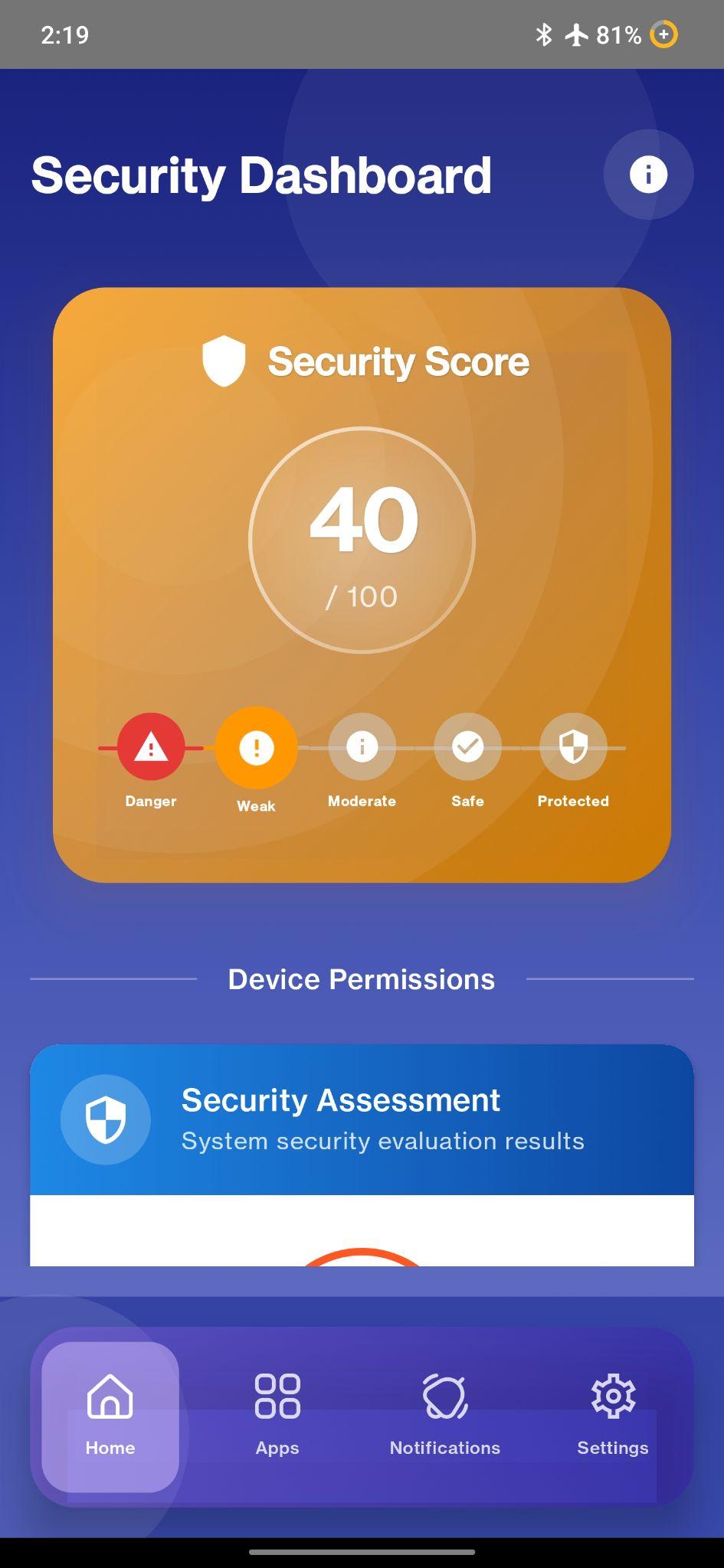
TRACKO

1.

In this section, we elaborate on the methodology used in designing, developing and testing the proposed mobile security system. The system incorporates three core segments under which a few other sub-segments are present. These core segments include a User Incentive Phone Dashboard, Real-time Tracking and Categorized permission system. The system is proposed to be built using Kotlin and Java for Android. We aim to put this system forward as a default phone system. This way we endeavor to achieve a technically feasible, effective and economical before expanding and putting these features forward into user testing. We work towards raising awareness among mobile users about their privacy in the digital world and take proper steps to mitigate these issues using our user incentive mobile security system app. For the time being, we are working on an Android-based app, but we also aim to enter the Apple store as well.

**1.1**

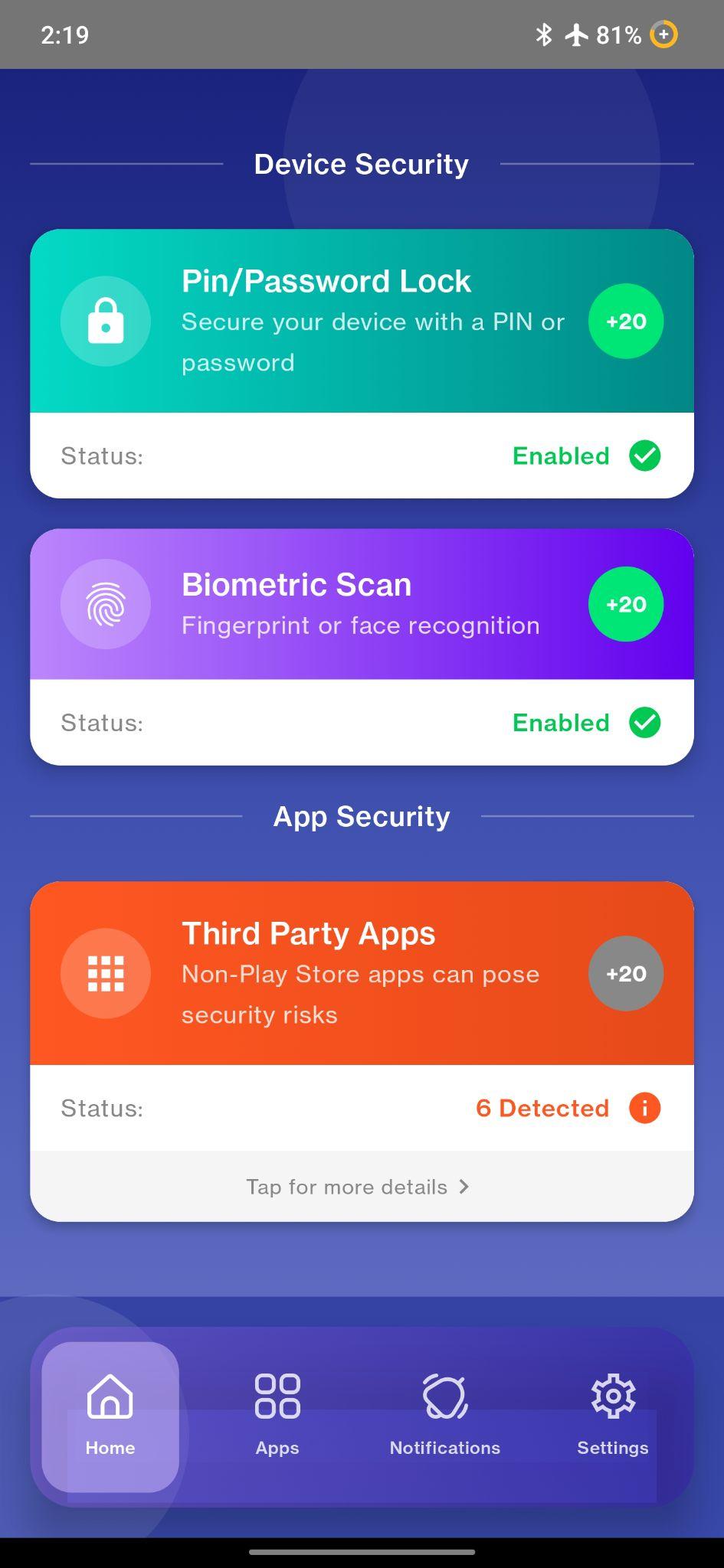
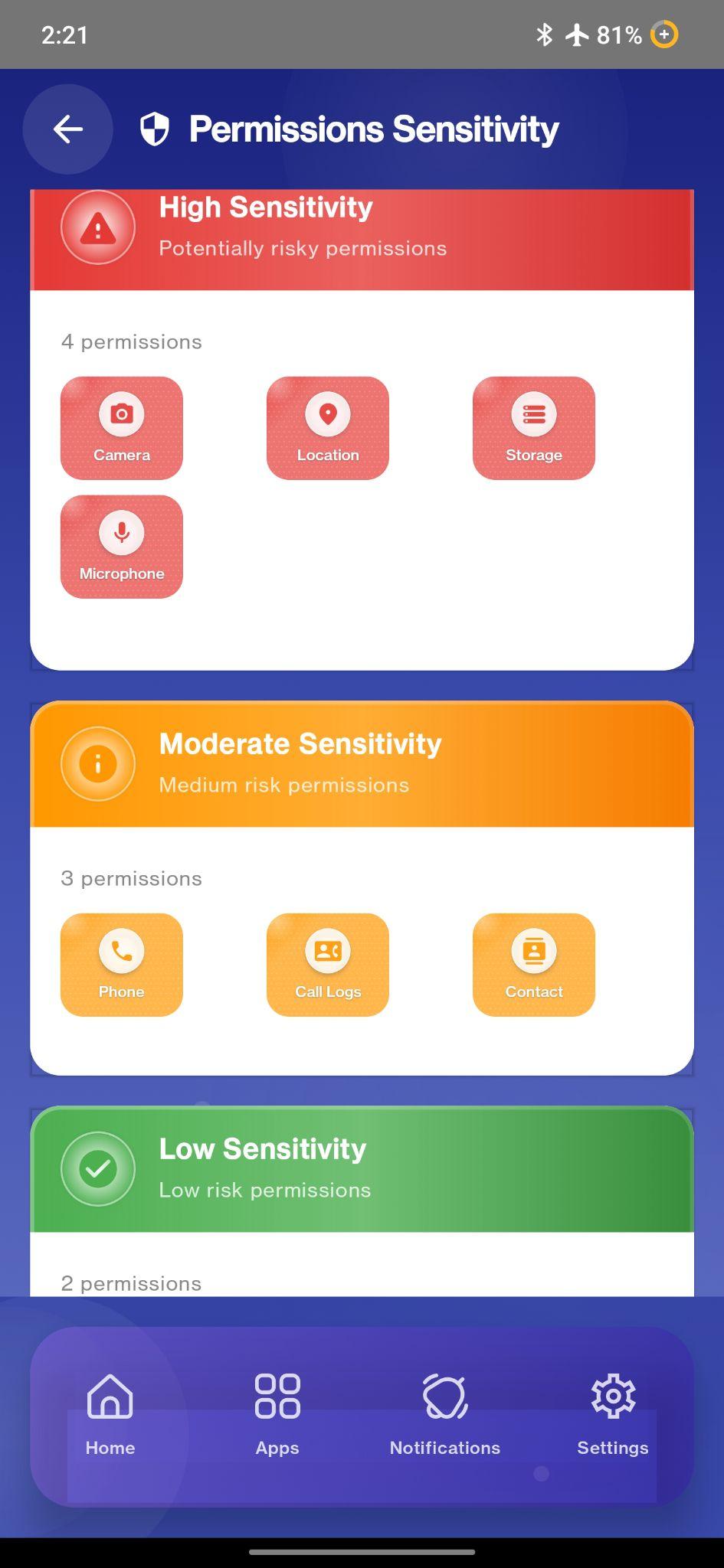
**System Design and Architecture:**

The app will provide users with control over their phone. It will provide a sense of security and also ensure the privacy of the user while using their mobile device. After downloading an app, the app will be automatically categorized into preset app categories and provided with the subsequent permissions. When the downloaded app uses any other functions other than the preset ones, the app will send a notification to the user notifying the user of unauthorized access to certain functions. The user may then either give access to the app to use the function or get rid of the app. The app provides real-time notification of any unauthorized access of any apps on the phone using real-time tracking. It also increases user incentive to ensure their data security and privacy by implementing a point-based system. The design of the system is user-friendly and customized in easy language for non-technical users with easy accessibility. 

**1.1.1 Phone Incentive Dashboard:**

The phone Incentive Dashboard is the central interface of the app, providing a point-based system for user incentives where users can earn points by fulfilling a few security and privacy-ensuring steps, which thereby ensures the user's privacy and maintains security while using apps. The point-based system uses the following security checks to provide points to the user and incentivize the user to ensure mobile security.

The activities that are included in this reward-based system are as follows:

1. **Phone Password:** This segment ensures whether you have given a password for your phone or not. According to a 2018 Kaspersky Lab study, more than half of people don't password-protect their mobile devices. The system provides 20 points to the user for using passwords to protect their phone. Usually, these passwords include patterns, passwords, and PINs. When a user activates one of these passwords and thus initiates secure behavior, the app also incentivizes the user by rewarding them. When a user's phone is not protected by a password or security lock, the system diminishes the user's points by 20 points. 
2. **Biometric Lock:** Biometric lock systems are a more secure way to protect one's phone data and provide security. Nowadays, all smartphones have a biometric lock system. While PINs, passwords and patterns can be cracked, biometric systems provide more security. The biometric lock system includes a Retina scanner, Face ID, and Fingerprint. When a user activates the biometric lock system on their phone, the system rewards them with 20 points. Subsequently, when a user doesn’t use a biometric lock system, the system decreases the user’s points by 20.
3. **No Third-Party Software:** This function is to encourage users to download apps from only the Play Store or Apple Store, rather than downloading from third-party software. Usually, third-party software can access one's account by simply downloading the app. Whereas the Play Store or the Apple Store has security features to prevent such privacy breaches. To ensure no third-party access user is rewarded with 20 points.
4. **Sensitivity**: The functions of the device that require permissions and may acquire threats are identified by the application. These functions are divided into 3 segments by default according to the sensitivity of imposing threats. These are:
5. High- allotted 60 points and has direct live tracking threats
6. Moderate- allotted 30 points and has indirect tracking threats
7. Low- allotted 10 points and threats are not that severe.

These segments have been by default, arranged with functions and allotted points to these. The user will be able to drag the functions from their respective order and migrate to another according to their choice. The points will adjust readily and with sensitivity as well. This change can be conducted from the settings section of the app.

The marks gained within 100 will be converted to 40%. The details of this calculation are done in the scoring assessment section.

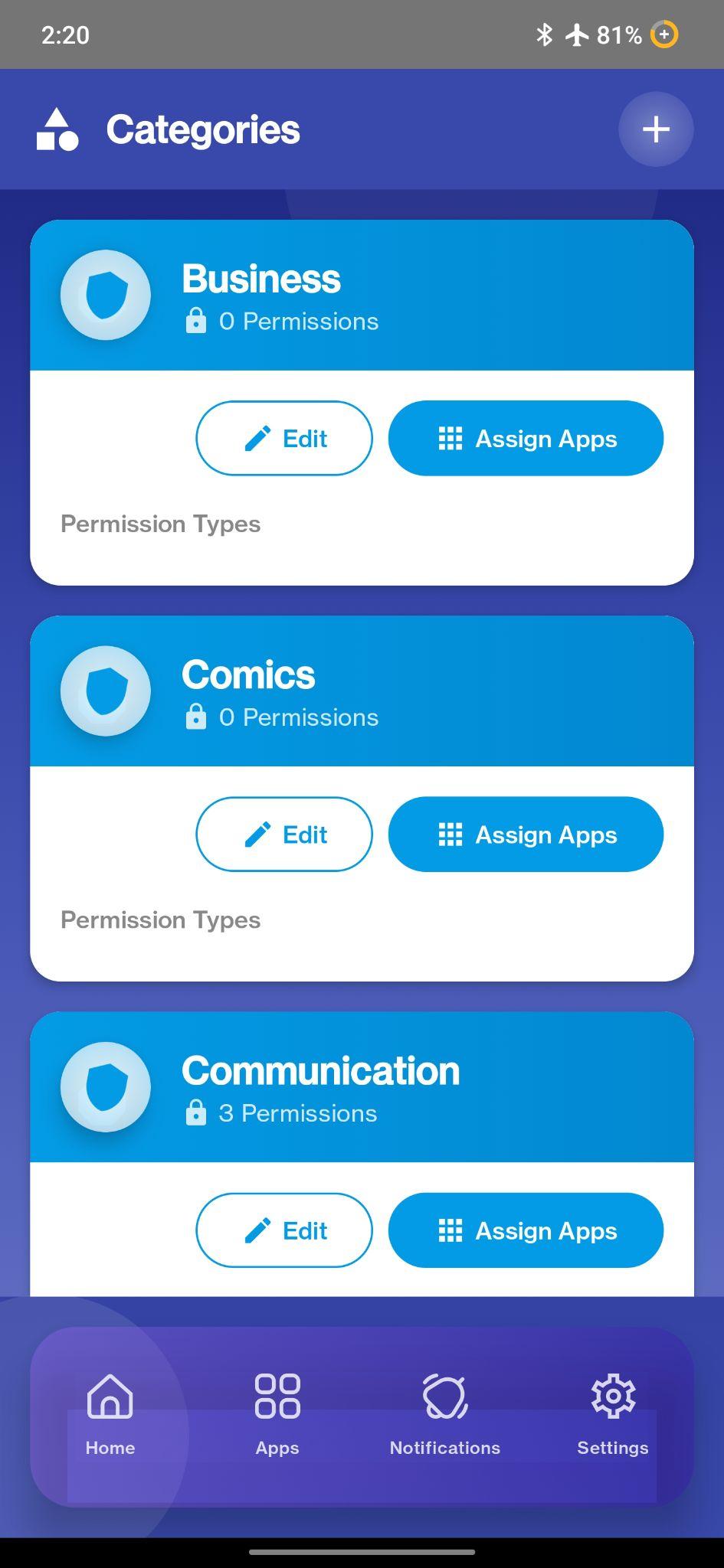
The idea behind this Phone dashboard interface is to encourage users to increase their phone security using a point-based reward system as an incentive.

**1.1.2 Real-Time Tracking (Not Implemented):**

This function of the system uses real-time tracking operation to monitor the downloaded app’s behavior and determine the accesses that these has over the phone's functions. It constantly tracks the installed apps for any unauthorized access and notifies the user of the app's unusual behavior, thereby alerting the user of his/her privacy being breached. The system function monitors whether the app is using the phone’s camera, microphone, gallery, contacts, files, Location/ GPS, etc. The very moment an app wants to interact with any of these resources, the system sends a pop-up notification to the user informing them of the app's security breach. It is a plus point that the system doesn’t drain the battery at a higher rate and also doesn’t interfere with the device’s performance. The notification is also written in simple language and in an informative notion. The user can invoke permission for the app at any time and also allow permission to the app at any time.

**1.1.3 Categorized Permission:**

The system has pre-declared and set apps in different categories. According to this category of the app, different apps have different sets of permissions already declared in the system. Thus, any app, when installed, gets assigned to these categories and thus a set of permissions is already given from the system. The user can customize the app’s categorization. The user can also add new categories and determine which permissions will be required in general and arrange apps within. Users can create categories for apps so that they can specially categorize any app of their preference and customize the permissions required for that particular app in question.



Our suggested categories are (Default) :

1. Weather: This app includes apps that have predictions of weather, earthquake etc, according to location.

Allocated permission: Location

Examples: Weather Forecast, My Earthquake Alerts etc.

1. Video players and editors: This segment includes apps that are used for photoshopping or editing pictures or videos.

Allocated Permissions: camera, microphone, gallery

Examples: CapCut, Filmora etc.

1. Travel: This segment includes apps that give ride services, air tickets, hotel bookings etc.

Allocated Permissions: location

Examples: GoZayaan, Grab, Booking.com, Airbnb etc.

1. Tools and Utilities: This segment includes apps that can be used as operating software and VPN’s.

Allocated Permissions:

Examples: RAR, Secure VPN, AppLock, SHAREit etc.

1. Sports: This segment includes apps that are used for game updates.

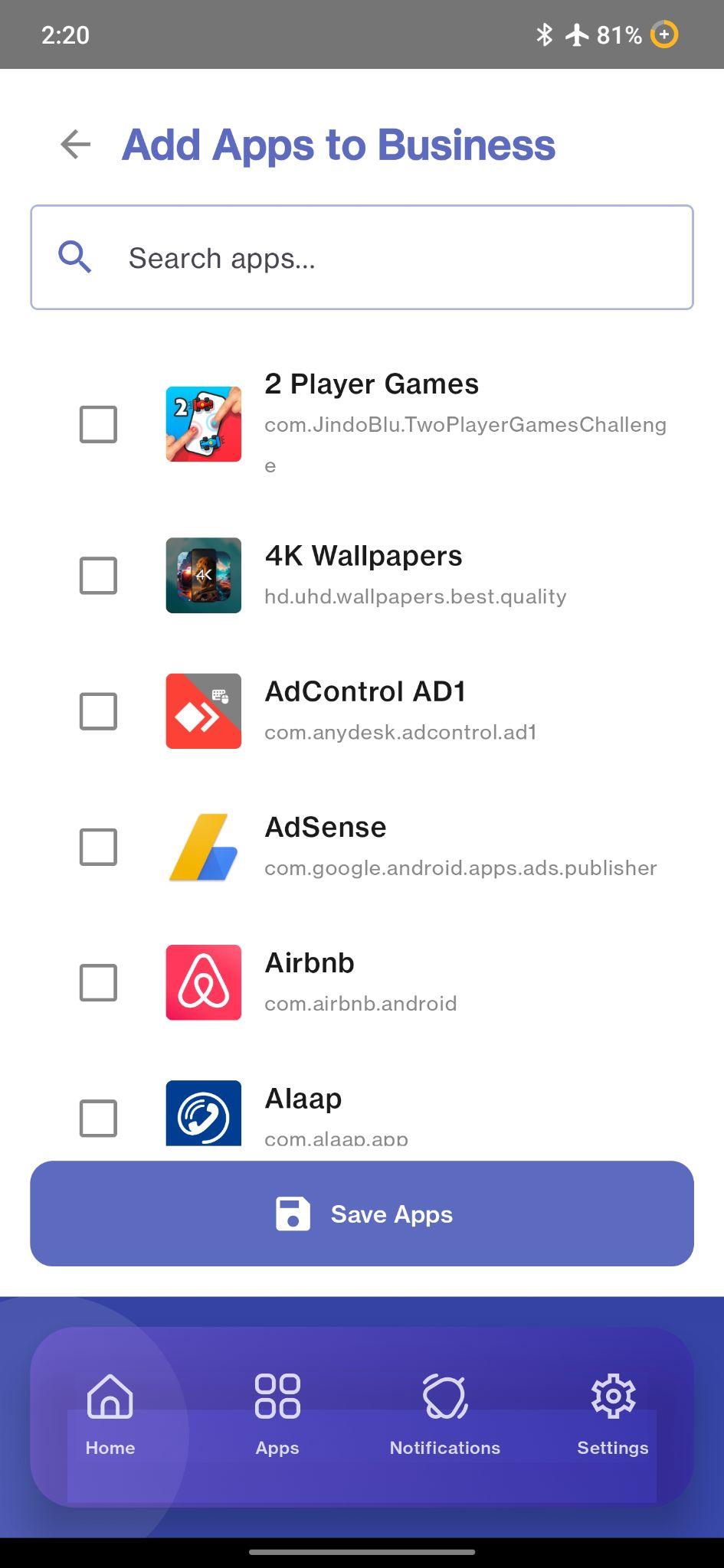
Allocated Permissions:

Examples: Cricbuzz, Cricket Line Guru etc.

1. Social media: includes all sorts of social media platforms.

Allocated Permissions: gallery, files

Examples: TikTok, Instagram, Facebook, Reddit etc.

1. Shopping apps: Includes all kinds of online marketing apps.

Allocated Permissions:

Examples: Amazon, Meesho, Daraz, Ali Express, Flipkart etc.

1. Productivity: includes apps that help in everyday studies, management etc.

Allocated Permissions: files, gallery

Examples: CamScanner, Chatbot, Microsoft etc.

1. News and magazines: this segment includes all the news and magazine apps.

Allocated permissions:

Examples: BBC, CNN, The New York Times etc.

1. Maps and navigation: includes all the navigation-related apps.

Allocated Permissions: location

Examples: Pathau, Uber, JoyRide etc.

1. Medical: Includes all the medical service apps.

Allocated Permissions:

Examples: Shukhee, MedEx, DocTime etc.

1. Libraries and demo(e-books) : Includes all kinds of online reading apps.

Allocated Permissions: files

Examples: Holy Quran, Holy Bible etc.

1. House and home (Alexa, Google Home) : Includes home assistance apps.

Allocated Permissions: microphone

Examples: Home Security Camera, HelloTask etc.

1. Health and fitness: Includes fitness and health-related apps.

Allocated Permissions: Bluetooth

Examples: MyFitnessPal, Calorie Counter, Step Tracker etc.

1. Games: All kinds of actions, strategic, online, offline, adventure games are included.

Allocated Permissions:

Examples: Mobile Legends, Candy Crush, Angry Birds etc.

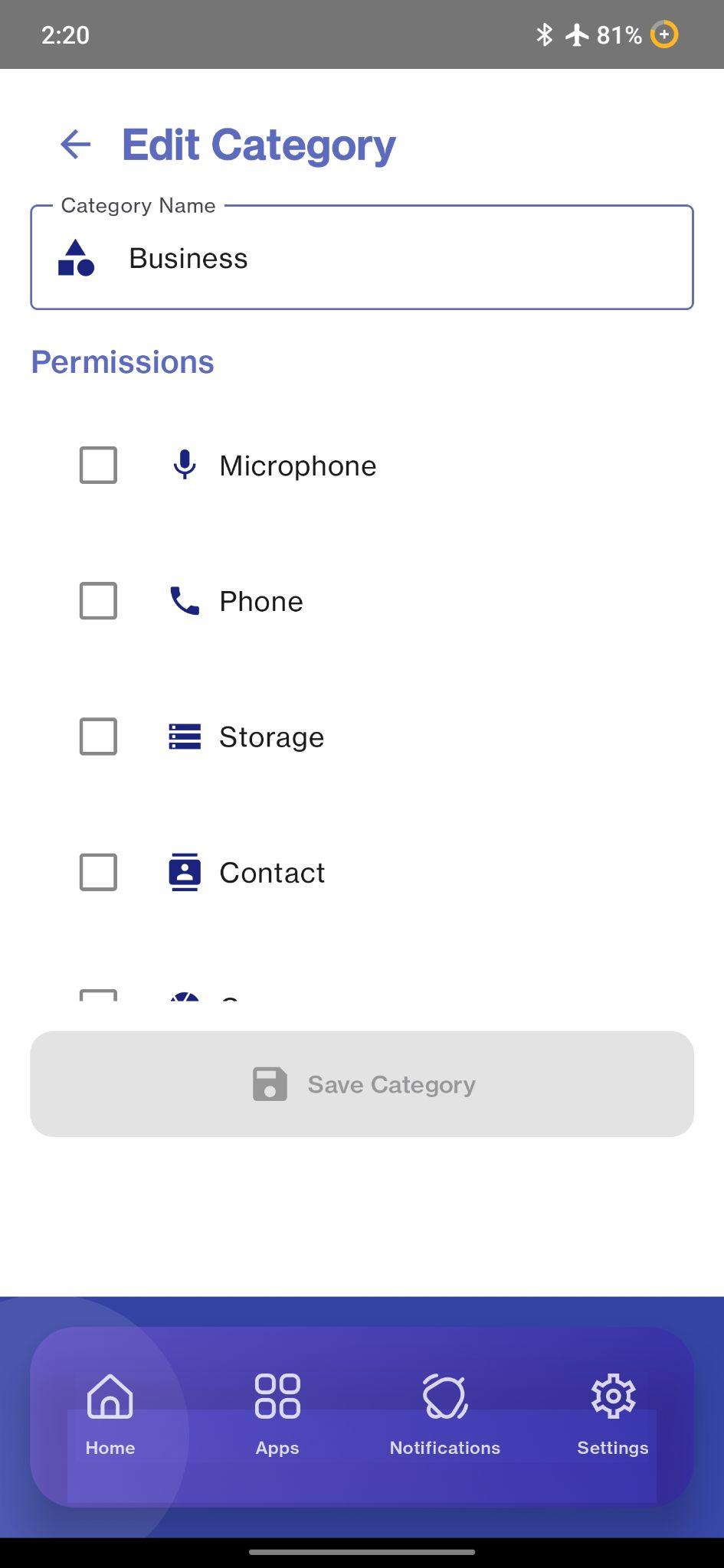
1. Food and drink: Includes food delivery, food review apps.

Allocated Permissions: location

Examples: Foodpanda, Food, Uber Eats, Zomato etc.

1. Finance: All forms of money management, Wallet organizer apps, Online money transfer apps are included in this segment.

Allocated Permissions: Contacts

Examples: Money Manager, Monefy, bKash, Nagad, Rocket etc.

1. Entertainment: All forms of entertainment apps are included in this segment.

Allocated Permissions:

Examples: Sony LIV, Netflix, Toffee, Bongo, Amazon Prime etc.

1. Education: This segment includes online education platforms, academics helping apps etc.

Allocated Permissions:

Examples: Photomath, 10 Minutes School, Duolingo, Khan Academy etc.

1. Dating: Includes all sorts of online dating or relationship-forming apps.

Allocated Permissions: gallery, location

Examples: Tinder, Bumble, Flirtify etc.

1. Communication: Includes all types of online communication apps.

Allocated Permissions: microphone, camera, gallery, files

Examples: Imo, Messenger, WeChat, Skype, Whatsapp Business, Viber etc.

1. Comics: Includes apps that are usually manga or comics etc.

Allocated Permissions:

Examples: MangaHub, WebToon, Tapas, Wattpad etc.

1. Business: All kinds of business-affiliated tools and apps are included in this segment.

Allocated Permissions:

Examples: Freelancer.com, UpWork, Zoom Workplace, Meta Business Suite etc.

As we do not have access to the Google API, we still haven’t categorized all the apps. We aim to target most of the useful apps into categories.

**1.2 Development Process:**

The creation of the mobile security system is done using Kotlin and Java

has the capabilities of supporting both Android and iOS. However, at this stage, it

is an Android exclusive app development with the intention of later adding the

iOS platform. The development takes an iterative, progressive model where one

starts with the basic functionalities by prototyping and then gets to the base of the

development by implementing these chief functions after which one optimizes for

working conditions.

**1.2.1 Prototyping:**

The development process starts with prototyping the key features of the system. This is necessary to understand the layout, problems and how the program would actually work if formed properly. This phase includes the development of the Phone Incentive Dashboard, the Categorized Permission System and the Real-Time Monitoring System. The Phone Incentive Dashboard includes the point-based reward system’s application by displaying whether the phone’s password, biometric control, password change and third-party access are protected or not and subjects the respective part to a point accordingly. The dashboard includes the total points accumulated after. This point’s system is designed to be dynamic as any and every change made in the respective user’s security changes, the dashboard is configured to be updated accordingly. We ensure the proper workability of the phone’s incentive dashboard and point system by developing the prototype.

**1.2.2 Implementation of Live Monitoring (Not Implemented):**

Usually, Android APIs have a tendency to access sensitive resources such as the camera, GPS and microphones. The live monitoring system is implemented to monitor any API access to these sensitive resources without authorization. The feature becomes active by running in the background and monitoring all the APIs. When an API uses any unauthorized resource, the system monitoring in the background detects the irregular use of the resource by that specific API and the user is notified by our pop-up notification system immediately. As the user is notified immediately of the API and the resource they are using, it is real-time.

**1.2.3 Implementation of Categorized Permission Warning System:**

This system is built based on the categorization of apps and presetting the recommended resources as permissions allocated. The apps are categorized into 23 different categories, such as business, weather, dating, games, health and fitness etc. Although the Android Play Store has thousands of apps, for prototyping, we have included only 23 categories and a few of the apps. In the final app, the system will have almost all the categories and apps along with a few sub-categories for a better user experience. Then we designed a configuration system that when an API is installed, categorizes the app into one of our set categories and analyzes the permissions set for that particular category. The system then provides the API permissions to use only the recommended resources, thereby ensuring the user’s privacy and security. When the API uses any unauthorized resources, the real-time monitoring system alerts the user using the pop-up notification feature. The user can also customize the permissions of the intended app by just getting into the app's category and selecting the app. The system lists all the authorized and unauthorized permissions to resources. The user can select or deselect any resource from the permissions board that has a very attractive interface for maximum user experience..

Limitation:

1. Real-time Tracking: Our app incorporates a function to track in real-time whether any application is trying to access any critical resources. The complication is that it is not possible to conduct this function by the app itself. It is a function implemented by the operating software of the device. Only if we get access to the operating software of the device itself will we be able to incorporate this function within the app.
2. Changing Password in 1 week: Our application incentivises users to change their passwords once a week to maintain a high level of security. The operating software of the device doesn’t allow the application to be notified of the change of password for a week. As the application isn’t notified of whether the password was changed or not, the function within the application remains ineffective.
3. Manually select Category: For the time being, we have to select and categorize apps ourselves. In the future, we hope to access the Google API to automatically categorize an app as soon as it is downloaded.
4. Limited Additional Permissions: Currently, our application can show whether our apps can access wifi, Bluetooth, keyboard, and internet. Although many functions can be seen, our application only focuses on these 4 functions. We expect to broaden our horizon in the future.

**Scoring assessment:**

The scoring assessment of the application is categorized into 5 sections, such as-

1. Danger: 0-30
2. Weak: 30-50
3. Moderate: 50-70
4. Safe: 70-90
5. Fully Protected: 90-100

Each accumulates different ranges of points. We carefully placed a high range in the Danger option to incentivize the user to ensure bare minimum security. The next 3 sections are in the range of 20, which is lower than Danger but higher than the range of fully protected. We then added a range of 10 points in the Fully protected section. This low range is to make it difficult for the user to achieve a perfect score.

The application is designed to reward users with 60 points for ensuring and acknowledging the warnings. The remaining 40 points are rewarded based on the security assessment devised by the application. This way, the user has to ensure security on pin/password lock, biometric lock, 3rd party access etc, early on to achieve points. After achieving the 60 points, the user will then have to acknowledge the security warnings to clear up those threats and achieve the rest of the points.

Points in the 60 point range will be given only if there are no security threats for that definite function.

Sensitivity:

1. The functions of the device that require permissions and may acquire threats are identified by the application. These functions are divided into 3 segments by default according to the sensitivity of imposing threats. These are:
2. High- allotted 60 points and has direct live tracking threats
3. Moderate- allotted 30 points and has indirect tracking threats
4. Low- allotted 10 points and threats are not that severe.

These segments have been by default, arranged with functions and allotted points to these. The user will be able to drag the functions from their respective order and migrate to another according to their choice. The points will adjust readily and with sensitivity as well. This change can be conducted from the settings section of the app.

**Scoring assessment:**

For a better understanding of the point assessment, the following table is given:

| **High-60 points** | **Moderate-30 points** | **Low-10 points** |
| --- | --- | --- |
| Microphone-15  Camera-15  Storage-15  location-15 | Phone-10  Contact-10  Call loga-10 | Nearby devices-5  calendar-5 |

In Table 6.1, we have explained 3 different levels of risk assessments: High, Moderate and Low. The values in them are the functions at risk being threatened. The functions are described below:

1. In every column of Table 6.1, the total points are fixed as long as there is at least one element present in that column.
2. If a column in Table 6.1 is void of elements, the total points allotted for that column will be divided among the rest two columns. For example, if the low risk column is empty, then 10 points will be divided into two 5 points allotments and added to the high risk and moderate risk columns.
3. For each column of Table 6.1, the elements will have equal points divided by the allotted total points for that column. For example, if the moderate risk column has 5 elements in it, then each element will have 6 points allotted to it.
4. After the total points from each column are added, the numbers are converted from 100% to 40%.

Interview Process:

The interview targets potential users from different educational backgrounds, genders, and ages to ensure inclusivity of all forms of experiences. The interview is specifically divided into two segments. The questionnaires are prepared ahead of time before the execution of the interview process. The interview is conducted in 4 different steps.

Stage 1:

In this first stage, random potential users will be given the app for use without instructions for 5 minutes with supervision in one of our sample devices. This is to understand the issues a user might face while operating our app. It will also enlighten us on the complexity of the app’s design. After 5-10 minutes, we ask our potential users what they understood from the app and what problems they faced.

Stage 2 :

In this stage, we help the user to download the application on their device. Then we note down what the current score on the device of the user is. We instruct the user on how to use the application. We explain in detail how the permissions and categorization of downloaded apps work, how the sensitivity of different functions of the device is at risk and how they can manage to ensure the safety of their personal data with our app. We share a detailed elucidation on how the point system works and how to increase their score in our app. After that, we part with the user for a duration of 1 week. Before parting, we provide the potential user with our contact info to contact us if they face any issues while using our app and also provide a descriptive video on how to navigate the app for a better understanding of the user.

Stage 3:

After 1 week, we analyze the score they achieved on their device. We then inspect the changes in behaviour of the user, their change in view regarding safety concerns of their data while using a device.

Stage 4:

At stage 4, we conduct an interview. This interview is to see if the user’s view towards their personal data, safety concerns, and ease of using our app has changed.

The interview would be compared to understand how much the user is incentivized to ensure security of the device and data, user-friendliness of the app and improvements suggested. We compare the points of the application in the user's device and the initial sample device that the user worked on in stage one. This helps us to understand the points to be improved, fixed and upgraded.

Interview Design :

The questionnaire consists of the user’s personal information, several questions divided into types, such as

1. Quantitative- System Usability Scale(SUS), Ease of Use(EOU)
2. Qualitative- Permission Categorization System, Point and Reward System, Ease and Learnability, Behaviour and Privacy Awareness, Overall Feedback

Demographic questions in a questionnaire are fundamental for understanding your audience and providing context to the data you collect. They are used to gather basic, factual information about the characteristics of your survey respondents. We have used a few demographic questions in our app.

The System Usability Scale (SUS) is a standardized, widely used, and reliable questionnaire that provides a quick way to measure the **perceived usability** of a system. This aims to quantify subjective opinions. The SUS is administered in our interview to users after they have interacted with our app. It uses a 5-point Likert scale ("Strongly Disagree" to "Strongly Agree") for each of its statements.

Ease of Use (EOU) is a fundamental concept in user experience and usability. EOU questions in our interview are to directly assess how easy or simple users perceive our app to be. We use Likert scales (e.g., 1-5, from "Strongly Disagree" to "Strongly Agree").

SUS questions we included with a Likert scale were

1. I would like to use this app regularly
2. I found the app easy to use
3. I think I would need help to use this app
4. The features were well arranged
5. I had to learn many things before using it

The EOU questions with a Likert scale were

1. The permission alerts were easy to understand
2. The app helped me understand which permissions are necessary
3. The point system encouraged safe behaviour
4. The dashboard helped me stay aware of my phone’s security
5. The customization settings were easy to use

Qualitative questions are used in our interview to evaluate user’s experience, learnings. We have separated the qualitative questions of our interview into 6 sections, where each section accommodates 3 questions for the user. These questions were asked verbally to the user and their answers were recorded as out data. The sections are as follows:

1. Permission categorization:
2. What did you like most about the permission alert feature?
3. Was anything confusing or unclear in the alerts?
4. Did any app’s permission alert help you take action?Please give an example.

B. Point & Reward System

1. What was helpful about the point system?
2. Did it feel motivating to earn points for good security habits?
3. Did you find anything unnecessary or confusing in the point system?

C. Customization and Settings

1. Did you try customizing permission categories in settings? Was it easy or hard?
2. Did assigning apps to categories from settings save you time?
3. What was your experience with the sensitivity customization(drag and drop)?

D. Learning and Usability

1. Did you need a tutorial to understand how the app works?
2. Which part was the hardest to understand?
3. How can you make this app easier to use for you?

E. Behavior and Awareness

1. Has your attitude toward app permissions changed after using this app?
2. Do you feel more in control of your privacy now?
3. Has this app made you more careful about which apps to trust?

F. Overall Experience

1. Which feature did you like the most and why?
2. Which part of the app needs improvement in your opinion?
3. Would you suggest this app to others? Why or why not ?

### **RQ4 – How would our proposed app secure user’s device privacy?**

Our proposed app ensures user’s privacy by executing functions that actively detect, notify and incentivize users to maintain the security of their personal data and information. It addresses probable digital security threats through real-time monitoring, permission categorization and a point-based incentive system. These functions work together to ensure user’s awareness of security threats, limit unauthorized access and encourage users to secure habits.

The real-time tracking function in our app is a cornerstone in privacy protection. Though it is not yet implemented fully due to OS limitations. It is designed to monitor any apps’ unauthorized access to users' data and sensitive resources. As the app notices these threats, it actively notifies users of the invasion through a pop-up notification system. The sensitive resources include camera, microphone, location, contacts, call logs, gallery, files etc.

The categorized permission system of the app is added for the user’s ease of categorizing apps based on their security preferences. This system allows users to restrict and allow certain permissions of their choosing to selected apps. This reduces the risk of unnecessary exposure of data and puts the control of data in the user’s hands. They can categorize apps, create categories and assign a variety of permissions on functions and restrict the rest.

The app also includes a home incentive dashboard, which transforms user’s secure habits and security threats into a quantifiable and teachable task management system. The user’s avail points when responding and mitigating the security threats encountered. While ensuring the safety of their data by setting up a phone password or pin, biometric lock, avoiding third-party apps and removing unnecessary permissions to apps, the user is granted points. This incentivizes users to complete tasks and avail points. This not only helps users mitigate existing security threats but also ensures long-term behavior change in secure habits.

Also, by ensuring the drag and drop system of permissions between sensitivity levels( high, moderate, low), the app promotes user control, making the user feel invulnerable with their information. The dynamic scoring system updates in real time to changes and threats made either by the user or by other apps. This scoring system allows an instant and dynamic picture of the device’s security.

Despite the already strong groundwork for privacy protection the app provides, we are still working on providing OS level access and full automation of app categorization. As mentioned in the system design, we aim to integrate GOOGLE APIs for automatic categorization and expand the scope of monitored permissions beyond Wi-Fi, Bluetooth and internet in future updates.

In conclusion, the app ensures long-term behavioral change in users, Real-time transparency and active security from unauthorized access and security threats. It empowers users to control their data and monitor these in real-time. This approach manipulates users' views on privacy and makes it worthwhile, user-friendly and rewarding to ensure proper security of their device and data.