TRACKO: Boosting Mobile Security through User Incentives and Privacy Controls

by

Nafiz Ahmed Rhythm
21301581
MD Rezaul Karim
21301019
MD. Shamsul Haque Sakin
22241174
Asif Imtiaz Chowdhury
21241050
Fatema Tuz Zohora Panna
21301456

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
Brac University
January 2025

Declaration

It is hereby declared that

1. The thesis submitted is our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

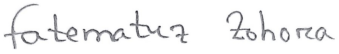
Student's Full Name & Signature:

Nafiz Ahmed Rhythm
21301581

MD Rezaul Karim
21301019

MD. Shamsul Haque Sakin
22241174

Asif Imtiaz Chowdhury
21241050



Fatema Tuz Zohora Panna
21301456

Approval

The thesis titled "TRACKO: Boosting Mobile Security through User Incentives and Privacy Controls" submitted by

1. Nafiz Ahmed Rhythm (21301581)
2. MD Rezaul Karim (21301019)
3. MD. Shamsul Haque Sakin (22241174)
4. Asif Imtiaz Chowdhury (21241050)
5. Fatema Tuz Zohora Panna (21301456)

Of Spring, 2025 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on June 20, 2025.

Examining Committee:

Supervisor:
(Member)

Dr. Farida Chowdhury
Professor
Department of Computer Science and Engineering
Brac University

Program Coordinator:
(Member)

Md. Golam Rabiul Alam
Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Dr. Sadia Hamid Kazi
Associate Professor and Chairperson
Department of Computer Science and Engineering
Brac University

Abstract

With smartphone upgrading, it results in the enhancement of mobile security tools. Nevertheless, the majority of users do not adhere to simple privacy practices, leaving them exposed to threats, such as malware, phishing, and unauthorized access to their data. Options like PIN locks, fingerprint sensors, and app permissions are underused not as ineffective ones but simply because users are either unaware of them or fail to find the necessary motivation. This mismatch between what is available and what is used by users is where we start our research. In order to gain a better grasp of what users care about and what keeps them from using security features, we started with a survey of 363 participants. Our goal was to understand actual user patterns—how they actually handle app permissions, which security tools they may like and how much control they feel they have over their privacy. The results demonstrated that most users want simple, easy-to-understand tools that not only alert them about risks but also guide them in making smarter decisions. Based on these findings, to ensure mobile security, we developed a mobile prototype named TRACKO that placed emphasis on both usability and engagement. The prototype includes two core features. Firstly, a categorized permission system analyzes the access each app wants to what is normally needed for that type of app (for example, a calculator asking for location data) and immediately notifies users about anything that is not necessary. Secondly, a system of rewarding points where users can earn points through secure behavior, such as setting PIN passwords or biometric locks, denying third-party app installation and managing app permission sensitivity. People who are careful about security get points for doing these things, which makes privacy more like a game. We then tested the prototype with 41 real users for one week and conducted a semi-structured interview. The evaluation showed promising results. Users understood permission-related risks with having a change of their behavior—taking more control over app permissions, adjusting settings they had previously ignored, and becoming more careful overall. In short, when security tools are made more transparent and rewarding, people are more likely to use them. This study highlights that improvement of mobile security is not just about increased functionalities—it is about designing experiences to help everyday users to make safer choices.

Keywords: Mobile security, App Permissions, User Behavior, Privacy Awareness, TRACKO, Categorized Permission System, Reward System, Usability, Prototype Evaluation, Behavior Change

Table of Contents

Chapter 1

Introduction

The smartphones have become a usual part of our lives. People use them for much more than calling or texting. Today, we store personal information, manage bank accounts, send emails, and stay active on social media through our phones [27]. Although such features are useful they also have serious security and privacy implications.

As time flies, the number of mobile apps has grown up, especially on Android devices by platforms such as the Google Play Store. Many of these apps are made using reused software components, and 61% of 110 studied apps included low-quality libraries that made them less secure [28]. Some apps ask for access to things like contacts, location, camera, and microphone—even when these are not needed. Research shows that 78% of health and wellness apps shared user data with other companies, but most users did not know this because of unclear privacy policies [63]. Another study found that 24% of the permissions requested by Android apps were not relevant to what the app is supposed to do [34].

Although phones today come with strong security features like encryption and fingerprint locks, many users do not use them properly. Studies show that 86% of users do not fully understand mobile security, and many give unnecessary permissions or ignore important updates [42]. Also, 1.8% of health apps were found to have harmful software like trojans, and nearly half of these apps did not use secure communication channels, putting user data at risk [63].

As apps get more complicated, people often give permission to access personal data without realizing it. For example, a flashlight app may ask to use your microphone or access your contacts. Most users agree without reading carefully, which leads to their personal data being collected unnecessarily [62].

Similar concerns have been raised by previous studies as well. Enck et al. (2014) created a tool called TaintDroid to track how apps handle user data and found 68 cases of misuse from just 30 apps [23]. Felt et al. (2012) and Lin et al. (2012) found that users often do not understand what permissions they are giving to apps, and some developers use this for advertising or other purposes [10][15]. One survey showed that only 17% of Android users checked permissions when installing apps, and just 3% could answer questions about permission use correctly [11].

Another serious issue is that some apps continue to use permissions like the microphone or GPS even when they are not open [16]. Even though phones have security options, many users do not take steps to protect themselves. They skip updates, use simple passwords, and do not turn on features like two-factor authentication. Even people who understand technology sometimes ignore these steps because they think the risks are low or the setup is difficult.

To make things worse, hackers are finding new ways to attack. Now, phishing does not just happen through emails. It also comes through text messages, social media, and fake apps. Since 2009, more than 5000 security problems have been reported in the Android system [70]. This shows that we can not depend only on phone makers or app developers to protect us. Users also need to play a role by being careful and using the tools available to them [63].

One big challenge is that people do not often use the security tools available on their phones [42]. Many users are unaware and many others simply do not feel involved. For this, a system that keeps people updated and gives simple actions to follow is needed.

1.1 Research Problem

In our research we focused on addressing the issue of weak user involvement in mobile security. We also noticed that accessing unnecessary data is allowed by many users. For example, a photo editing app might ask for GPS access or microphone use, which has nothing to do with its main function. If users are not careful, this opens the door for apps to collect private information and even misuse it [16].

Many users do not review app permissions after installing them. They allow everything the app asks for, without understanding what it means. For this reason, they might unintentionally share too much information with apps and put themselves at risk. This is not only a technical problem, it is also a behavioral one. People need better tools and motivation to stay involved in managing their phone's security.

A categorized permission viewer and a point-based reward system- these two main features combined in this research to introduce a new mobile security system.

In the categorized permission feature, permissions for apps like camera, location, storage, contacts and microphone are arranged into categories. It compares each app's permission requests with the kind of app it is. If an app asks for something unusual, the system highlights it. For example, if a calculator app asks for access to your microphone, the system will flag this as suspicious. **This helps users understand what permissions are needed and what are not.**

The second part of the system is a point-based reward feature. Users will earn points for doing safe actions, such as setting up a screen lock, using fingerprint or face unlock, and avoiding apps from unknown sources. These points are shown in a

security dashboard that gives a "score" based on how safe the phone settings are. **The idea is to make security habits fun and encouraging.** Studies show that giving people small rewards can help them build better habits—this works well in health and education and is expected to work for mobile security too [37][44].

This combined system is designed to **help users in two ways: it gives clear information about app behavior, and it motivates users to take actions** that improve their phone's safety. Many security apps focus only on blocking or detecting threats, but our approach focuses on helping people stay aware and make better choices. Our aim is to improve mobile security by making it simpler, clearer and linked to users' daily behavior.

To check how well the system works, we will collect feedback through surveys and interviews. This will help us understand what users think about the features and how it changes their behavior. In the end, we hope this system can **reduce careless permission sharing and make users more active** in protecting their own data.

1.2 Research Questions

In this thesis, the focus is on understanding how users can be empowered to take a more proactive role in securing their mobile devices. The proposed solution aims to combine permission-based warnings, sensitivity-based categorization, and a point-based reward system to improve mobile security practices. The following research questions guide this study:

- **RQ 1:** How much control does an average smartphone user have over their personal data?
- **RQ 2:** What are the current user's perspectives/awareness of the permissions apps use in smartphone?
- **RQ 3:** What solutions exist to protect user data from privacy thefts, applications gaining unwanted permission access and spyware used for malicious purposes, as well as encouraging users to engage with privacy security? What can be proposed to resolve all the aforementioned problems at once?
- **RQ 4:** How would our proposed app secure user's device privacy?
- **RQ 5:** How does a point-based 'phone health dashboard' and reward system influence user behavior in adopting secure practices, such as sensitivity control, setting passwords and avoiding third-party apps?
- **RQ 6:** What are the usability challenges and user acceptance levels of a point-based security system that integrates unnecessary permission warnings and sensitivity controls?
- **RQ 7:** How will user's lives improve or be impacted or become more secure after using our app?

1.3 Research Objectives

In this research, the main aim was to understand how people deal with mobile app permissions and how we could help them stay more secure through a tool they would actually want to use. To begin with, we tried to learn how much control users really have over their data. We did not just depend on existing research, we went out and asked real people directly through a survey. This helped us to get a better understanding on how much users know about app's permissions, and whether they take steps to manage them or just leave the default settings untouched.

We also wanted to know how users feel about app permissions overall do they notice what an app is asking for? Do they say no when it is too much? And do they really understand what those permissions mean? These insights helped us to know where people are unsure or confused, and to make them feel more in control and confident of their privacy, what kind of guidance or tools could help.

After looking at a variety of existing tools and apps, we noticed that most of them either offer basic privacy settings or try to warn users, but they do not really help people form good habits. For that we built a prototype app which integrates several features together—alerts when an app asks for something unusual, categories for app types, permission sensitivity levels, and a point-based reward system to keep users engaged.

Once the app was ready, we asked real users to try it out for a week. During this time, we observed closely to see how they behaved to the alerts and the scoring system. Would earning points make them more aware? Would they change their behavior denying more permissions or uninstall risky apps? These were things we wanted to understand through real usage.

We also spent time observing how easy or hard the app was to use. Some users became comfortable with the system almost at the very beginning, while others needed a little more time—especially when figuring out how to adjust settings or make sense of the points system. Their honest feedback was helpful in identifying areas where we could make things easier and more intuitive for the people who are not used to customizing these types of features.

We also wanted to see if using the app made any real difference in how people think about their privacy. A lot of participants expressed that they now pay more attention to the app's permissions, and in making decisions about what to allow or deny they feel more confident. That response told us an important thing—our app did not just explain privacy. It helped people form better habits over time.

In the end, all we did, from understanding how people currently handle privacy, to building and testing the app—came down to one simple aim, to make mobile privacy easier to understand and more practical for everyday users.

1.4 Thesis Structure

We have arranged the rest of our research paper in the following chapters:

Chapter 2 (Literature Review): This section reviews previous research on mobile security, app permission management, and real-time notifications. It discusses user control mechanisms, categorized permission warnings, and incentive-based approaches to improve security practices. The chapter identifies existing gaps in security solutions and positions the research as a novel approach that integrates both real-time alerts and reward systems.

Chapter 3 (Methodology): This chapter describes the way our research approach is set up from the literature review to the conclusion. It covers the survey from the design to the data analysis, from understanding user control over mobile security to designing a solution to address their issues. It also explains our plan for the development of our proposed mobile security app and the app testing strategies. This methodology ensures that the security application is data-driven and effectively addresses mobile security concerns.

Chapter 4 (Survey Design): This chapter describes the survey methodology used to assess user perspectives on mobile security. It covers:
1. Demographics of respondents (age, occupation, smartphone usage, gender, location).
2. User practices and concerns about app permissions. Awareness and engagement with privacy tools.
3. Survey distribution methods, including online forms and physical QR codes.

Chapter 5 (Survey Results): This section presents findings from the survey, including:
1. Demographic Analysis – Majority of respondents were young adults, students, and urban dwellers.
2. User Perspectives – Many users rarely check app permissions, but there is growing concern over data privacy.
3. Privacy and Security Solutions – Interest in real-time monitoring and incentive-based security measures was high among respondents.

Chapter 6 (Developed Solution: TRACKO): The development for the solution focuses on designing, implementing, and optimizing the app "TRACO". The system is developed using Kotlin and Java for Android devices. The development follows an iterative progressive model, starting with prototyping, followed by implementation and then refinement. Also the features and how the features work and implemented is also explained in this chapter.

Chapter 7 (Evaluation via User Study): The steps of the user testing process outlined in the chapter include stages that are clearly defined and have various participants to test the usability, the effectiveness of the app, and its effect on the behavior of the people. The participants were introduced to the app by exploring it on their own and after one week, demonstrated to use it on personal devices.

Subsequently, their security scores and behavioral changes were determined. There were post-usage interviews, which were used both to gather quantitative results using SUS and EOU survey and qualitative feedback as an in-depth interview took permission management, point system, customization, usability, privacy awareness, and overall experience. The results were used to evaluate the strengths, weaknesses, and opportunities of improvement which the app had.

Chapter 8 (Discussion): A final detailed discussion about our whole research. The research question we defined earlier is properly answered and in which part of the research we found the answer is properly discussed in this chapter.

Chapter 9 (Conclusion): The final chapter summarizes key findings and discusses the implications for mobile security. It highlights the effectiveness of combining real-time alerts with user incentives and suggests future research directions, including expanding the system for iOS and refining the user experience to avoid notification fatigue.

Chapter 2

Literature Review

This chapter reflects the studies in this context of main concepts, findings, practical issues, and trends in the field of our research. By drawing a synthesis of prior researches, this chapter aims at providing an understanding of the current study in relation to the current scholarly discourse on the topic, and explaining its relevance to the field.

2.1 User Control via Real Time Notifications

The real time notification of suspicious app behavior is meant to raise the level of user awareness and to give users back the power to decide who they give access to their data and under what circumstances. Mobile devices can help users make decisions to allow or block access to sensitive information, such as location or camera, by informing users in real time when an application attempts to access it. This contrasts with traditional approaches where users might only realize after the fact. Felt et al [10] showed that users tend to change their app settings when they receive real time alerts that remind them what data is at risk and by whom. By alerting users when apps access unnecessary permissions (e.g., a media app accessing GPS), real-time notifications help prevent potential misuse or malicious intent. These systems work to prevent threats instantaneously before any harm can be caused to the user.

While real time notifications increase transparency, they also introduce the possibility that users will get overwhelmed with too much information, resulting in 'alert fatigue' [6]. If users are frequently made aware of such data access without clear, contextual explanations, then they could become desensitized to the alerts and start to ignore or even disable them altogether. In a sense, Fagan and Khan [38] noted that the relevance and clarity of these alerts are key elements for preventing user fatigue. Mobile security systems, however, need to find an effective balance: notifications need to be reserved for actions that actually impact user privacy. Not only does this prevent users, it also makes them eager to learn how applications make use of the data that they request access to and security protocols that help protect their privacy. So the transparency of real time monitoring and notification systems encourages users to actively engage in managing app permissions and data access, fostering a sense of control and responsibility over their digital privacy.

How users understand the information provided also determines how much user control real time notifications provide. Lin et al [25] research indicates that users often do not understand security warnings, especially those containing technical jargon. Messages that are clear and explain the possible risks of application behaviors such as sharing location data enable users to take more action on setting their privacy. Raising user awareness regarding threats to their privacy through nudges, according to Almuhimedi et al [31], made them rethink the choices they make when it comes to providing permission. A significant number even restricted suspicious applications accessing their data. So if the lack of user knowledge on data privacy is a potential cause for the problem, then alerting them of any threat to their sensitive data as soon as it occurs in real time provides an effective resolution.

2.2 Usability Challenges and User Acceptance of Integrated Security Systems

An integrated mobile security system that includes live monitoring, real-time privacy controls, and user incentives presents both opportunities and challenges. The usability of such systems contributes to their effectiveness, as complex interfaces or overwhelming features can discourage user interaction. Studies indicate that users tend to avoid interacting with security systems that they considered too complex or techy [4].

The live monitoring system gives you transparency of the app behavior, alerting you to possible risks as they happen. However, the continuous flow of information can lead to users being overwhelmed, especially for non-technical users. As Lillo et al [6]found that users often disable monitoring systems that provide a large number of notifications, reducing the effectiveness of the system. Additionally, users may have trouble interpreting the warnings and security alerts that these systems generate, particularly if the alerts are too frequent or not sufficiently explained.

According to Felt et al [7] the more the information is presented in a straightforward, intuitive manner, the higher the user acceptance of live monitoring systems. For example, systems should not bombard the users with technical details about what the app is doing. Instead systems could offer simplified summaries, such as "This app is accessing your location in the background. Do you want to continue allowing this?" Mobile security systems can enhance user acceptance and encourage utilization of more active security settings through minimization of technical complexity and providing actionable options.

Study by Liu et al [26] found that developers creating apps for Android systems are allied to request for over a hundred and thirty various permissions that programs can access. Reviewing and adjusting settings for all these permissions for all the applications that are used is rather illogical and simply not feasible. The results of the study suggest that, while people's mobile app privacy preferences are diverse, only a handful manage to significantly simplify the decisions mobile users have to make. Thus if we want users to remain in control of their data and prevent anyone

with malicious intent from accessing it under their noses, simplifying their options when any cynical activity takes place is the key to this.

2.3 Sensitivity Based Permission Alert System

In recent years, user privacy and data security have emerged as crucial issues owing to the proliferation of third-party programs soliciting unauthorized access to sensitive device functionalities. Our app resolves this issue via a point-based permission alert dashboard, which is intended to inform users anytime an application accesses sensitive device components, such as the microphone or location services.

We established a sensitivity-based categorization system to enhance the evaluation and management of app permissions. Each permit is designated a sensitivity level: High, Moderate and Low according to its potential security risk. High-sensitivity permissions are ones that present increased dangers to user privacy if misused. For instance, access to the camera, microphone, or contacts is categorized as high-sensitivity, but permissions such as calendar access are deemed less damaging.

Due to the absence of a globally recognized standard for identifying permission sensitivity levels, our categorization is shaped by previous research and user-centric viewpoints. Numerous research indicates that sensitivity perception differs among users, influenced by personal preferences and the context of permission usage. Consequently, our application provides customisability, enabling users to manually designate sensitivity levels of rights according to their own discretion or risk evaluation.

To assist users in visualizing their device's security status, we created a security Dashboard, segmented into three sections:

High Sensitivity: High-risk permissions are often granted unintentionally.
Moderate Sensitivity: Permissions of medium risk.
Minimal Sensitivity: Low-risk or widely accepted authorizations.

The dashboard indicates the number of unnecessary or excessive permissions provided across all installed applications. The approach produces a score that assists users in comprehending the overall vulnerability level of their device.

This adaptable, sensitivity-driven methodology corresponds with contemporary trends in permission management, which promote enhanced user control, transparency, and knowledge regarding the access of their personal data.

2.4 Categorized Permission based warning system

A permission warning system can effectively analyze app requests and highlight unnecessary permissions, thereby enhancing user awareness of potential privacy risks associated with applications. By clearly indicating which permissions are essential for an app's function versus those that may be redundant, such a system can boost

trust among users by making them more informed about the choice they make to grant access. Struse et al [18] indicates when users are provided with clear and comprehensive information about application permissions, they are more likely to adhere to security principles.

The study by Michael Lane [14] probes into the Android permission framework and assesses the efficiency of the framework in keeping an end-user informed about potential privacy issues that an application may cause. An end-user is presented with the permissions required during the installation of an application and, thus, appears to make an informed decision about an application based on the permissions it requires. Among the ten applications widely used, a number were found with permissions that can constitute threats to the information privacy of which most end-users probably are unaware. The permission framework is complex for end-users to comprehend; hence, it is difficult for them to figure out the possible risk an application may pose to information privacy and security. The majority of end-users tend to install the application without considering the list of permissions that it requests for. These findings indicate that there is a need for improved decision-support applications that can empower end-users to make more-informed choices about the privacy and security provided by applications.

Due to these issues, researchers have proposed models intended for the quantification of security risks of Android permissions and applications. Olukoya et el [56] analyze the risk of an app based on the permissions it requests, using a permission sensitivity index computed from a risky permission set. They evaluate permission mismatch by checking what an app requires against what it requests. They evaluate security rules based on our metrics to evaluate corresponding risks. They used the datasets of benign and malicious apps, 43580 apps, and their result demonstrates that the proposed framework can be used to improve the risk signaling of Android apps with an accuracy of 95%.

A model named DroidRisk aimed at permission system efficiency enhancement [21]. There has also been research into the risks of permission granting to uncover malicious apps, where detection rates as high as 94.62% are feasible at very low false positive rates [30]. These results are a motivation for increased user education and decision-support mechanisms and, arguably, much stronger privacy protection legislation.

However, Sarma et al [17] stated that it is crucial to understand that having excessive permissions may cause serious security issues. Apps that ask for too many access rights may allow malicious programs to gain access to devices. Such as weather forecasting apps may request for our location, but if they ask for access to the gallery or contacts, it may be a malicious program attempting access to our information and can expose us to risks like data breaches and privacy violations. Jutail et al [55] stated these intrusive programs pose a threat to users' privacy and general safety because they can track users' location, steal sensitive information, and monitor activities without permission.

Furthermore, applications that seek permission to access personal data—like con-

tacts or messages—can place users at risk of identity theft and financial fraud if these applications contain harmful or poorly designed code. In particular, when apps gain authorization to read phone status and identity details, these permissions are frequently ignored by users. Consequently, some applications may use this information to manage incoming calls while inadvertently exposing personal identification details through unique device identifiers.

Malleswari et el [46] stated that mobile devices contain sensitive information regarding their users. When applications are granted access to this information, there exists a risk of unconsented sharing with third parties for their advantage. Furthermore, these applications have the capability to consistently track the user and their activities. They often request permissions that are not fundamentally necessary, thereby facilitating the unauthorized acquisition of the user's data. It has been concluded that companies compromise users' private information through an Android app and permissions they ask for. As the user remains unaware of their sensitive information utilization while installing apps and granting permissions, this matter raises a serious concern about privacy. Thus, the authors demonstrated that there is a need for a risk assessment framework that could keep the users informed about the potential danger that an application poses to personal information. So, they proposed a method aimed at increasing user awareness of the privacy risks from granting permissions to Android apps. Alternatively, this model takes in consideration the permissions that an app is asking. It grants the risk based on the permission set asked for and gives a risk score in that regard.
Idris et al [52] demonstrated that mobile applications frequently access data beyond their rights and share it with other parties for a variety of objectives, such as marketing, profiling, and advertising. So they introduced a Privacy Enforcement Framework (PEF), which evaluates app permissions to improve privacy for Android users. By addressing problems like overly privileged programs and confusing permission requests, it offers users to find privacy-friendly apps and efficiently manage permissions, eventually encouraging wise privacy choices.

Sarma et al [17] also stated that users often overlook the implications of these permissions, leading to unauthorized access to their personal information. According to a study done by Microsoft, 90% of users simply click "yes" without even reading the terms and conditions regarding risk concerns of access permission. Felt et al [7]investigated the efficacy of application permissions on modern platforms such as Android and Google Chrome, emphasizing their benefits over conventional user-based permission systems. They claim that almost all apps—93% of free apps and 82% of commercial apps—ask for at least one dangerous permission, suggesting that consumers are used to installing apps with such permissions.

According to Yilmaz et al [72], the permission system is essential to the operation of mobile applications to control access to private information and protect system resources. Users are expected to make decisions regarding permission selections based on an app's features. Nevertheless, many users remain oblivious to the fact that some apps may grant extra permissions to unrelated entities. According to a recent study by Alenezi and Almomani [41], 80.3% of Android apps ask for more permissions than are required. Attackers are given the chance to carry out destruc-

tive actions, such obtaining private user data, because of the way the authorization system controls access to sensitive information. Furthermore, a lot of third-party libraries in the Android ecosystem need access to device data in order to gather personal information such as location, network status and MAC addresses[68]. Numerous spyware and viruses may take advantage of it, consequently, putting users' sensitive information at risk without their awareness. Thus increased user awareness about the nature of these permissions is crucial, as this can enable them to make more educated decisions about the access they choose to provide. This study therefore attempts to provide Permission Risk Signals in cases where permission requests appear fishy.

2.5 Reward or Incentive based User Engagement

Brower et al [57] investigate the ways that financial and non-financial incentives influence user engagement. Specifically, its goal is to provide motivation to perform such activities through reward in the form of points that can be redeemed to purchase groceries, travel, or entertainment by passing health quizzes; engaging in physical activities and availing public health facilities. The study shows that increase in reward size has an effect on employees' engagement but other factors like type and timing of the reward also contribute to the level of engagement. For instance, they found that users were more encouraged by real life rewards, like movie tickets, as compared to those that were more utilitarian, like gas points. Also, a large number of small rewards given in concrete connection with accomplishing tasks were more effective in producing sustained behavior compared to large isolated rewards. This goes with behavioral economics, where the notion of immediate rewards encourages a particular accomplishment. They also pointed out how the rewards pointed out by participants were successful to sustain engagement even though the size of the reward was less over a period of time and definitely also highlighted the contention that consistency and relevance of incentive are more important than its face value. Analyzing the success of the Carrot app proves that advocating for the use of non-financial incentives in health promotion interventions is possible.

Di Nocera and Tempestini [66] discuss the use of security and usability trade-off, a well-known issue whereby high security comes hand in hand with low usability and vice versa. So, instead of trying to remove such trade-offs, the authors suggest that one way to design for security is through the use of behavioral rewards for safe behavior. They say that such things are possible to implement where individuals are given different points such as points for the creation of strong passwords or not using default login credentials. These rewards could be blur interfaces, game-like concepts or more straightforward work processes that create a virtuous cycle where users are sensitive enough to want to practice good security. According to the research, users are more likely to use secure behaviors if they experience a positive motivation. For example, what if users could get points or badges for changing a password or even for doing it more often? It motivates both security and usability.

The work of Busch et al [33] addresses the pertinent issue of how to motivate employees to follow organizational security policies and standards which they might experience as inconvenient. Their solution is called Behavior Change Support System

(BCSS) that includes use of gamification and persuasive technologies for promoting security. The BCSS comprises six functionalities; Security Points, Quizzes, Challenges, Statistics, Personalization, and Risk Communication all of which are meant to incentivize the employees to interact with the security policies on the platform. The users can get points and badges for performing some security related activities like quizzes or achieving definite security objectives. They can also participate in tasks that involve rivalry with co-workers on feasible goals and this provides social comparison and organizational incentives. Although these rewards are given virtually they provide extrinsic motivation by satisfying the need of accomplishment and recognition within an organization. It is discovered that employees' use of the security policies improves if the framed security policies are portrayed as involving incentives as opposed to preventive measures. In this manner, the BCSS encourages organizations to enforce security, while at the same time, offering relevant feedback for compliance, and tracking user progress to keep them interested and productive.

Goel et al [58] conduct this study to examine the way financial incentive may help enhance security behavior in organizations. This speaks about the difficulties organizations experience in trying to enforce compliance with security measures among employees, mostly because they remain carelessly vulnerable to such threats. The paper is largely confined to financial incentives, to which various monetary incentives to achieve security measures among the users. One of the findings include the fact that although monetary incentives influence the behavior of the target audience in the interest of the organization in the long run there is lack of compliance because the behavior that was targeted, decreases when the incentives are withdrawn. These methods involving financial incentives and gentle suggestions gave encouraging outcomes as to the participants' password strength and their vulnerability to phishing, though the sample size was small and larger scaled studies were recommended.

Chen and Li [43] examine the determinants of security software use by mobile device users, with emphasis on privacy. The paper also incorporates the utility element, specifically the emotional incentive, anticipated regret which can lead to users clicking on protective software and downloading them. Even though they do not emphasize monetary incentives directly, they elaborates the role which perceived efficiency and efficacy play. Privacy threats combined with threats of future regret are made as appeal to emotion, as a means of prompting defensive behavior. The study goes further by claiming that within the preview of decisions to do with privacy and security, monetary incentives push people into action, but other factors such as regret seem to also influence action.

To evaluate the effects of monetary incentives in increasing user participation, Lu et al [50] experimented with an approach to understanding users' motivation to sign up and participate actively in activities relating to online car-sharing platforms. The actual field experiment was carried out that showed that monetary incentives in the form of coupons offering a discount were not much more effective than email invitations to complete the profile and book a car. By specifically focusing on digital platforms, the study shows that privacy concerns regularly act as factors which neutralize the outcomes of financial rewards. The authors said this means that financial incentives must be properly calibrated to user expectations so it does not

backfire or cause unintended side effects such as increasing privacy concerns of users.

The research work by Herath and Rao [2] examines the factors that could encourage workers to observe information security policies at the workplace. The study employs the principal agent model using incentives including fines and social compliance, and intrinsic motivations including perceived efficacy of the actions taken in security. According to the authors, certainty of detection weak positively while severity of penalties may have weak negative effect on policy compliance. They also raise awareness of social pressures whereby the employees are pressured by the demands of their colleagues or their bosses. Moreover, the study reveals that practical actions of the employees, is the belief in the efficiency of one's actions which, in turn, determine the level of policy compliance. This paper adds to knowledge of how improvements to penalty systems and favorable perceptions of the effectiveness of security can be used to increase desired, secure behaviors among employees within organizations.

The paper by Villamarín-Salomón and Brustoloni [5] provides information on how user behavior in reaction to security warnings can be enhanced using positive reinforcement. Instead of punishing poor security decisions the authors suggest using Security-Reinforcing Applications (SRAs) that would encourage users to make more secure decisions. The paper presents Vicarious Security Reinforcement (VSR) where in the case of Social Learning Theory is used to present users with how secure actions are positively reinforced by others. This research shows that sparse reinforcement, where users are rewarded occasionally, ensures that security is sustained beyond usage of the application. This approach proves that with positive motivation and with learning from the behavior of other people, the rate of maintaining security protocols for longer periods by users is enhanced.

The research of Lakshmi et al [64] shows the influence of the users by basing incentives on participants who share information and data through smartphones. However, users refrain from contributing to the creation of content because of privacy and lack of incentives to work for something that can be valuable to developers. To address this, the study will present two models of reward systems aimed at encouraging participation while preserving the privacy of the user. The first model involves credit dissemination by a TTP (Trusted Third Party) based on information from the users concerned. The second model which does not require TTP uses mechanisms such as blind signatures to ensure the anonymity of the users who receive the rewards which would have been misused to accumulate excessive credits. The credit-based incentives make many users engage in the platform's activity, and, at the same time, their data are not linked to them. Also, the rewards are designed to complement the concept of preventing dishonest workers with the possibility of their attempting to provide fake or duplicate information. The study shows that when incentives are tied to privacy assurances, consumers are indeed able to contribute long term to such collection endeavors.

In this paper, August et al [22] aims at explaining whether economic incentives are effective to motivate users to engage in enhanced cybersecurity. People sometimes neglect updates because of the hassle, like when a program or an operating sys-

tem requires patching, and may take time probing before notifying the user; they may take even longer time patching before alerting the user, hence users may never undertake the procedure. To encourage the invention of novel heuristics that can help reduce this behavioral gap, the authors present a versioning model. In this scheme of things, users could choose between a cut down version of the software that updates automatically and a full version that lets the user decide when to, or even if, to update. This strategy concerns user incentives with cybersecurity goals by providing the automatically updating version with lower price compared to the full license, thus giving more incentives for price sensitive users to choose the former, minimizing risks in the entire network. Companies that consider internet connectivity as mission-critical may opt for the premium version, but they are encouraged to update quickly due to consequences of vulnerability. This model recognizes that all users are not going to react the same way to security updates and institutes a system where external rewards are given according to preferences in order to achieve security objectives of a network. By associating the capability to postpone patches with a certain monetary price, the model guarantees that more few systems are unpatched and hence there are less exposed systems within the network and hence the resultant safer zones in the digital world.

This paper by Anderson et al [19] seeks to establish how badges can be used as incentive and reward that help in encouraging users as well as influencing their behavior in online communities. Through the use of these badges, seen below, users are motivated to continue with a task or attain a certain level or achieve detailed objectives in a platform. These rewards do not only serve as recognition of accomplishment but also remind users to contribute much more time and efforts to gain their badges. Since people are motivated to gain accolades and learn, achieve goals, and evolve, the information demonstrated by badges serves as compelling motivators encouraging users into completing activities they would have otherwise ignored or undermined. The paper goes further to describe how placing of badges at some important stages would help in maintaining the user engagement. Contrasting with competitiveness of leader-boards or external motivation as monetary incentives, badges appeal for the motivation of acknowledgment intrinsic to a community. This renders badges a versatile and non-comparative method of encouraging longitudinal as well as diverse engagement. The study shows how contemplating and managing badges, therefore, can greatly alter consumer behaviors and this makes badges a universal incentive mechanism that encourages broader use and specialized efforts within online communities.

This research by Bruggen et al [20] looks at how various incentive structures help to encourage improved security measures concerning smartphones, especially the screen lock mechanisms. The users in the study still included a large number who did not practice security measures at all, despite the fact that some form of security measure was in use by many of the users. To facilitate change, the researchers compared and tried different types of interventions; incentives appeal to moral selves and/or fear, and sanctions appeal to fear and/or self-interest. Incentives based interventions provided user practical incentives in form of points or benefits for user adoption or increased security practice. While such incentives led to some extent of shift in behavior, the result was not as dramatic as the researchers had hoped, and

significantly less efficient than the threat-based strategies that targeted the user's fear of possible consequences. The study shows that incentives may get people to change their behavior but it takes more than incentives to sustain the change. However, this research also points out that incentives are most effective when backed by social pressure, for example, peer pressure. It appeared that the perception of imitating security practices of others would make users act out similar practices. The research established that the rewards are useful means to encourage user participation, but when used in combination with other approaches like social encouragement and relentless training to maintain positive behavioral changes in the long run.

2.6 Users Control over Personal data

Research shows that people who use smartphones have limited control over and knowledge of their own personal data. According to a paper by Zhou [49], many approved applications access sensitive information without users fully realizing what is happening. Many authorized apps use sensitive personal data without users' knowledge. Smartphone privacy protection methods offer privacy settings to control leaking. Smartphone privacy settings warn consumers about privacy leaks and allow them to regulate their phones. Understanding and measuring user perception and trust in these contexts is crucial. A fine-grained online survey with 222 respondents is designed and conducted. They collect demographics and smartphone usage, including age, gender, employment, daily smartphone use, personal data relevance and sensitivity, and smartphone OSs. This paper examines smartphone users' current privacy perception and protection in different groups, including Rating the importance and sensitivity of personal information; Trust in existing privacy protection; Perceived smartphone control; Frequency of searching privacy knowledge; and Concerns about manufacturer and third-party company behaviors on personal data and decision.

Even though there are privacy options, consumers often have trouble comprehending and dealing with these limitations. A paper by Shakila Bu-Pasha [39] suggests that Smartphone location data collection and processing raise privacy concerns. These activities may violate EU data protection and human rights laws. Transparent steps to secure user privacy at all levels of smartphone usage and users should have some control over personal data associated with smartphone usage, including location, and that this control should be executed under a legal arrangement that secures users' privacy and allows app developers or operating system providers' lawful purposes. In order to address these difficulties, tools like My Data Store have been developed to improve users' understanding and management of their personal data. Initial findings indicate an enhancement in users' awareness of their personal data and the perceived utility of the tool [29]. According to recent research on Android privacy permissions, consumers often revoke access for programs that they do not use regularly or for features that are not critical. This typically happens within a short period of time [73]. The results highlight the need for privacy management solutions that are more clear, explicit, and user-friendly so that smartphone users may control their personal data more efficiently.

Yefim's research provides a conceptual analysis of personal information control to better understand and improve it. The findings also showed that people may assume that personal information can be learn from other disclosed data about them, placing it outside their control. It is important for system designers and privacy practitioners to advise users about information that may become public as other information is revealed. Further research is needed to understand how consumers construct perceptions and mental models of their abilities to regulate their personal information available to internet service providers [67].

Min Mun implies, increasing mobile phone use is creating many opportunities for personal context sensing, which will result in enormous databases of sensitive information such as locations, movements, photos, text annotations, and health data. Existing system architectures upload raw data streams straight to content-service providers, giving users little choice once they "opt-in". Hence they offered Personal Data Vaults (PDVs), a privacy architecture where users own their data. Data is screened before being shared with content-service providers, and users or data custodian services can regulate data sharing. This enables users flexible and granular data access management [3]. Despite smartphones being personal devices, the practice of sharing phones has demonstrated considerable popularity among users at various levels. Data access control is an alternate option that enables users to determine the extent to which particular information on their device is disclosed to specific individuals [40].

Liccardi I. et al [24] found three reasons why people are unaware of this. Firstly, it is easy to overlook important rights in long lists. Second, apps that need personal information to work might seem questionable, even if they can not share that information. Updates to apps can result in new permissions that allow them to view personal data. They compared the old and new versions of the interface and discovered that the better permission interface helped participants, especially those who were inexperienced, choose apps that gave less access to their personal data. Matina et al [36] assert that while granting access to smartphone users' personal data is inherently neither problematic nor illegal, contemporary smartphone operating systems fail to offer sufficient protection for users' personal information. Nonetheless, numerous concepts exist that can substantially enhance the circumstances and alleviate users' privacy concerns regarding smart devices.

2.7 User's Perspectives of the App's Permission

Recent research has examined consumer perspectives regarding application permissions on Android and iOS platforms. Users are increasingly controlling access to and sharing their data in various contexts, including mobile apps, cookies, and social media. However, many users struggle with informed permissions-related decisions due to a lack of understanding of permissions and interface issues. Despite privacy settings provided by web services, they often fail to capture essential considerations. Research suggests that end-users misunderstand permission requirements, highlighting a gap between knowledge, perception, and behaviors. As privacy decisions grow, it is unrealistic for ordinary users to manage all privacy settings [69].

Users typically exhibit a lacking in understanding the permissions utilized by their applications, thereby compromising security and privacy. The implementation of Android's runtime permission model by Peruma et al [51] has improved users' capacity to remember requested permissions. Nonetheless, a study by Scoccia [53] on Android's permissions-based security model revealed widespread permission-related issues, with 8% of apps having negative comments about permissions. The study analyzed 3,574 permission-related reviews from over 4.3 million users about 5,572 apps in the Google Play Store. Despite the new system, recurring points were identified, and recommendations for improvement were provided. The study highlights the need for further research to improve the Android run-time permission system.

The study by Tahaei [71] explores the reasons developers request permissions and their conceptualizations, comparing their perspectives with end-users'. It found that both groups share concerns about unnecessary permissions, potential damage to reputation, and sensitive data access. Developers sometimes request multiple permissions due to confusion, while end-users believe they are responsible for granting permissions. The findings could improve permission ecosystems. The paper by Wang [61] proposes a framework called SmartPI, which uses crowdsourced user reviews to understand why apps request permissions. The framework uses Natural Language Processing (NLP) techniques to identify functionality-relevant user reviews from noisy crowdsourced reviews. The results show that permission usage can be better reflected by user reviews than claimed descriptions of apps, bridging the gap between functionalities and actual app behaviors.

A study by Ramachandran [48] says that users of Android devices are asked to grant app providers access to device features, impacting privacy and security. However, low attention and comprehension of permission warnings have been identified. An online survey was conducted to understand users' reactions to differences in app permission information. Results showed that the presentation of permission information in devices causes concern and irritation for a majority of users, especially those with basic IT expertise. The study concludes that contextualization of app features and permissions needs improvement, especially for users with little IT expertise, and that further user permission information should be made available at different levels of granularity.

However, studies by A. Felt [12] suggests that, the effectiveness of Android's permission system in warning users about the risks of installing applications. Results show that 17% of users pay attention to permissions during installation, and only 3% can correctly answer permission comprehension questions. However, a minority of users show awareness and comprehension. The study recommends improving user attention and comprehension, and identifying open challenges. Nonetheless, The paper by Umair [60] examines privacy concerns in wearables like smartwatches, focusing on data protection, safety, trust, ethics, and cybersecurity. Two Amazon Mechanical Turk studies reveal that users lack understanding of cybersecurity risks, believe app developers misuse data, and hold developers accountable for data breaches. They also express unease with data usage policies and consider all private data susceptible to data breaches. The study also highlights confusion between usability and security, suggesting a need for reliable, secure, trustworthy, and ethical technologies.

According to Chia [9], third-party applications on web and mobile platforms often use decentralized control strategies, relying on explicit user consent for permissions. Community ratings are used to identify potentially harmful apps, but these ratings often reflect opinions about functionality rather than risks. A study of Facebook, Chrome extensions, and Android apps found that current community ratings are not reliable indicators of privacy risks. They discovered that free and adult apps request more permissions than typical. Another study by Kelly [13] conducted in two cities found that Android users generally view and read permissions screens, but not understand them. This is concerning as users are unaware of the security risks associated with mobile apps and believe app marketplaces test and reject applications. This results in users not being well prepared to make informed privacy and security decisions.

2.8 Existing Solutions to Protect User Data and Proposals

The popularity of Android has led to innovative and customizable apps that require user data for services. However, privacy concerns remain. Android's permission system is often misused, requiring unnecessary permissions. A study by Misra [65] proposes a privacy-preserving secure framework to prevent apps from stealing user data by restricting unnecessary permissions. The model uses collaborative filtering and frequent permission set mining algorithms to predict necessary permissions, interacting with the application and modifying permission data. Experimental results show the model protects user data and ensures proper application functioning. Smart-phone users often lack the skills and awareness for effective privacy management, leading to permissive settings and data over-collection. Solutions often require domain-specific, user-specific, or extensive attention. H. Elahi et al [54] proposes a non-intrusive, representative privacy protection framework to reduce privacy fatigue and promote democracy in privacy management by involving application providers, marketplaces, and end-users to fairly distribute responsibility.

Spyware is a significant problem for computer users, tracking user activities, providing targeted advertising, and engaging in undesirable activities. A study by N. Good et al [1] have limited success in explaining user behaviors contributing to spyware proliferation. An ecological study of users installing five real-world applications found that notice alone may not be enough to affect installation decisions. Users have limited understanding of EULA content and often regret their installation decisions. Privacy and security become important factors when choosing between applications with similar functionality. A standardized format for assessing options and trade-offs between applications may be helpful.

The mobile operating system market is divided into Android, iOS, and Windows Phone, with Android being the most popular. Privacy protection on smartphones is a complex issue due to the variety of sensors and increased usage frequency. To address this, J. Pennekamp [47] proposes extensions to existing permission management systems and nudging mechanisms to trigger user interaction for a more privacy-

friendly system configuration. The paper reviews privacy enforcing on smartphones and identifies no solution suitable for proper privacy enforcement while offering reasonable usability. It also highlights the shortcomings of privacy enforcement on smartphones, including usability, users' ignorance, and conceptual problems.

Smartphones, primarily using Android OS, pose significant privacy risks due to third-party software development. S. Singh [35] says that In recent years, smartphones and tablets have replaced PCs as the main computer device. Thus, smartphones may now store massive amounts of sensitive user data in addition to communicating. Its popularity also opens a new age of app development, resulting in millions of free Android apps on Google's Play Store. These apps cost money and require users to grant data access. Sometimes the permissions are important such as Google map position information etc, but most of the time they are unneeded and compromise user security and privacy. Considering these facts, the author suggested a computationally efficient system to improve Android user privacy and security in his paper. The proposed framework sends user-sensitive data in scrambled form for all applications, enhancing privacy for both tech-savvy and tech-nobs. It aims to provide secure services for Android users and is aimed at future expansion to cloud and Linux-based systems.

Nonetheless, smartphones are increasingly used for personal information storage and handling, but rogue applications pose a threat. Existing solutions have limitations in addressing privacy-violating apps. A new privacy mode, TISSA, is proposed by Y. Zhou et al [49] to enable users to control access to personal information and adjust access dynamically. TISSA has been tested on over a dozen information-leaking Android applications, demonstrating its effectiveness and minimal performance overhead.

However, A study by Almuhimedi [32] reveals that combining an app permission manager and privacy nudges can significantly improve smartphone users' privacy control. The study found that users reassessed their permissions after a week with the permission manager and 95% reassessed their permissions after receiving nudges. Android and iOS have been proposed for privacy enhancements.

Peter Hornyack [8] developed two privacy controls for Android smartphones that allow users to run permission-hungry applications while protecting private data. They retrofit the Android operating system to implement these controls, but faced challenges in preventing side effects that interfered with user-desired functionality. An automated testing methodology was developed to measure the impact of these controls on 50 popular and permission-hungry applications. The controls successfully reduced effective permissions for 66% of tested applications.

Nowadays, mobile applications have become a significant source of personal information, exposing consumers to potential misuse. Despite advanced sensors and privacy controls, mobile operating systems often leave users unaware of how applications use granted permissions. A solution, SPEProxy by Krupp [45], aims to raise awareness of data misuse and protect users' data. This knowledge-based approach is device and operating system agnostic, allowing users to use the solution without technical

expertise. SPEProxy was found to be highly effective across 86.55% of popular iOS and Google Play applications.

2.9 Our Work

Our work stands out from other research highlighted in our literature review by uniquely combining real time privacy controls with a point-based reward system to enhance mobile security. Unlike earlier studies that typically focused on either increasing transparency with real-time notifications or motivating user behavior separately, our approach brings both elements together into a unified strategy. By doing so, we not only alert users about sensitive permission accesses but also actively encourage them to adopt better security practices through a structured incentive system. The dual approach addresses the gap between user awareness and engagement with security features, ensuring users can control their data and maintain long term behavioral change. Our research seeks to close the gap by identifying privacy risks as they happen and encouraging users to actively respond to these alerts, helping them take a more hands-on approach to mobile security. Table 2.1 shows a comparison of our app Tracko and the similar existing app we found.

Feature	**Tracko**	**TaintDroid [23]**	**PermissionWatcher [18]**
Privacy hook placement	×	✓	×
Unnecessary permission detection	✓	×	✓
Permission-based risk assessment	✓	×	✓
Static analysis of permissions	×	×	✓
Runtime monitoring of permissions	×	✓	×
User assigned permissions	✓	×	×
Dynamic permission management	✓	×	×
Categorizing apps into distinct classes	✓	×	×
Measure overall security	✓	×	×
User friendly UI	✓	×	×
Compatible with latest Android versions	✓	×	×
Compatible with iOS	×	×	×

Table 2.1: Comparison of Our App Tracko with TaintDroid and PermissionWatcher

Chapter 3

Methodology

This chapter describes how our research is planned and conducted to better understand user behavior and awareness regarding mobile phone security—especially focusing on app permissions, real-time notifications, and user incentives. The purpose of this chapter is to give a clear road-map of the steps we took, starting from identifying problems through literature, designing a survey, planning our proposed system, and evaluating its future potential. Our methodology aims to ensure that our research is data-driven, user-centered, and practically implementable in real-world mobile environments. Our overall approach is mixed-method: combining both qualitative and quantitative research techniques. This means we are not only interested in numbers and statistics but also in people's thoughts, habits, and preferences. The chapter establishes a foundation that links the previous literature review to our practical research. Subsequent chapters, including those on survey results and system development, will be predicated on the structure and outcomes outlined in this chapter. Figure 3.1 shows our methodology diagram.

3.1 Research Structure

Our research is organized and structured. This is meant to help us get from understanding what users want to the end evaluation of our proposed system. This method makes sure that each step of the study process is consistent and relevant, so that each stage builds on the one before it. The plan is made up of the following important steps:

1. Understanding Problem through Literature Review: To learn about what has already been done, find gaps, and shape our study questions.

2. Survey Design and Distribution: To get real-life information and data from users.

3. Data Analysis and Pattern Identification: To find patterns in behavior, attitudes, and wants.

4. Solution Design (TRACKO App): To make a mobile security system that is focused on the user.

5. Evaluation via User Study: To figure out how useful and important the system is by getting structured comments from users and watching how they act.

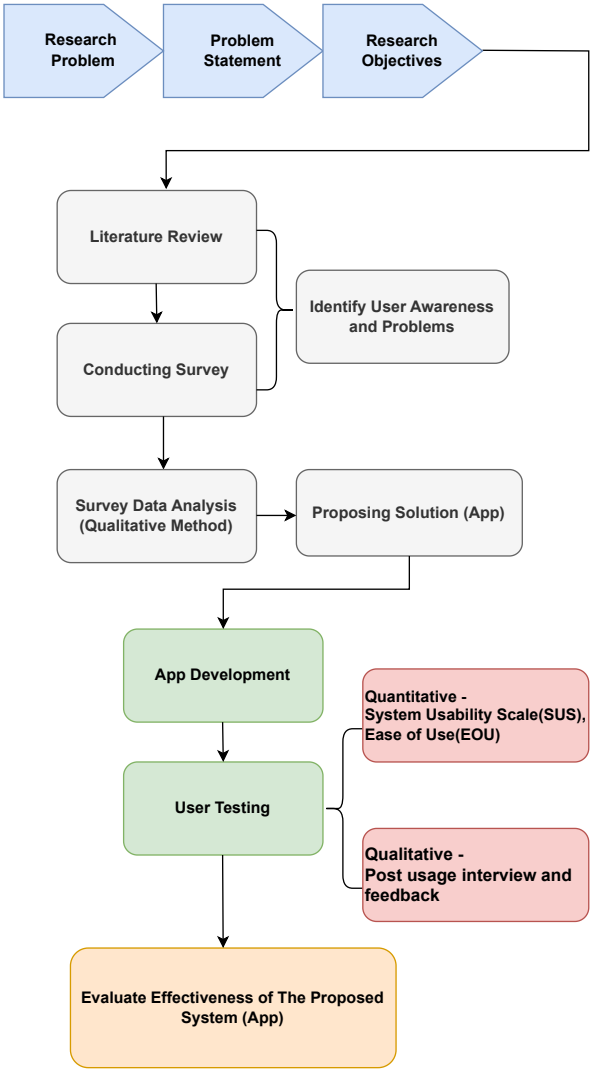


Figure 3.1: Methodology Diagram

3.1.1 Understanding Problem through Literature Review

Before creating any instrument or conducting any survey, it is important to have a comprehensive understanding of the problem's scope. In order to accomplish this, we initiated a detailed literature review that enabled us to pinpoint critical failings in current mobile security protocols.

We have observed in previous research that users frequently grant unnecessary app permissions without understanding the potential dangers. Numerous individuals are unaware of the implications of these authorizations or the potential for their abuse [14]. Mobile systems provide permission managers and other tools; however, users are unlikely to interact with them unless they are highly motivated [42]. This behavior gets taken advantage of by spyware and malware, which silently accumulate sensitive information.

An additional critical finding is that the lack of user engagement frequently results

in the failure of existing solutions. Even though there may be security apps out there, they will not help if people are unaware that they are easy to use or do not feel connected to them. Because of this difference, we looked into both a technical and a behavioural answer. This method encourages users to be more involved by rewarding safe behaviour and sending real-time tips. Our methodology was built on top of these findings. It became clear that we needed the following:
1. A clear picture of how users act and how they feel about giving apps permission to do things.
2. Find out what types of features people want in a mobile protection system.
3. In answer to these needs, make a system that is both friendly and motivating.

3.1.2 Survey Design and Distribution

The survey is divided into three major sections:
1. Demographics and Usage: Age, gender, occupation, and daily phone usage.
2. Behavior and Awareness: Questions on app permission habits and security actions.
3. Preferences and Expectations: User interest in features like instant alerts, educational tips, and reward systems.
The structured flow enables respondents to initially contemplate their own behaviors and subsequently consider the types of solutions that would either reinforce or modify those habits.

3.1.3 Data Analysis and Pattern Identification

The subsequent phase of our research involves the analysis from the survey to derive valuable insights, following the collection of survey data. This analysis functions as a conduit between the design of our mobile security system and user data. Analysis will include the following:
1. Quantitative Analysis: Utilizing statistics, diagrams, and charts to identify patterns (e.g., the frequency with which users verify their app permissions).
2. Qualitative Analysis: The process of examining open-ended responses to gain insight into the motivations, perspectives, and concerns of the individual.
3. Pattern Recognition: The integration of both forms of analysis to identify common themes in user behavior and expectations.
Through this step, we aim to identify, Gaps between awareness and action, motivational barriers that stop users from taking security measures and user preferences that can shape effective mobile security features. The findings from this phase will directly influence the features we prioritize in our app development.

3.1.4 Solution Design (TRACKO App)

We designed a privacy preserving monitoring system that prioritizes proactive privacy protection, ease of use, and motivation, as indicated by the patterns and preferences identified in user data. The application is intended to satisfy the precise requirements that are evident in user behavior. The application will comprise the subsequent essential elements:
1. Permission Monitoring and Categorized Alerts: Immediate, context-sensitive notifications when applications require access to high-risk permissions.

2. Smart Categorization: Arranges app permissions according to their relevance to the app's functionality.
3. Incentive Dashboard: Provides users with incentives for secure actions, such as disabling unnecessary permissions or employing biometrics and gaining points from it.
In addition to prioritizing functionality, the design endeavors to be habit-forming and educational for users who may not otherwise engage with security settings as frequently. In addition, we made sure the app works on all Android devices and meets usability standards before it is evaluated by users.

3.1.5 Evaluation via User Study

To ensure the systematic assessment of the usability, effectiveness, and general user experience of the suggested application, a user testing strategy was planned. The aim of this strategy was not only to evaluate the functional potential of the system, but also to measure its influence that could be had towards user behavior, user awareness of the need to have privacy, user experience of ease in using the system not only through the objective measurement, but also through the subjective response. The test design involved controlled observations, longitudinal usage and structured interviews involving both quantitative and qualitative designs.

Participant Recruitment and Sampling

The sampling method used was purposive, to make sure the variety of participants was broad, and hence the range of experiences and ability among them. Several demographic groups were recruited such as differences in educational levels, gender and age. This sample heterogeneity made it more thorough to evaluate the usability of the application based on different user profiles and this made the results more generalizable.

Multi-Stage Testing Procedure

The user testing was done in four different yet inter-related phases with each phase aimed at capturing certain dimension of user interaction and system performance.

Stage 1: Initial Exploratory Interaction (Unassisted Use)
During the first stage, the sample device on which the research application was availed witnessed a condensed testing duration and no form of instructions was issued to the participants. This step was supposed to provide a first impression as well as to see the navigability of the system by intuition. Observational data were recorded to find out the barriers to usability, design complexities, and any complications when using it upon the first time usage. After this interaction, the participants were invited to tell about their direct perception of the purpose of the app and report about the problems that occurred.

Stage 2: Guided Setup and Independent Use (Supervised Installation and Familiarization)
The participants later installed the application on their personal devices under the supervision of the researchers. It was explained in detail how the system works in

terms of granting and refusing permissions, adjusting the sensitivity levels of the permissions, and the reward-based system of the incentive mechanism implemented to encourage people to follow the privacy-friendly behavior. There were also educational materials like instructional videos and written manuals to help the subjects feel sufficiently supported in the first set of independent usage. They were then left to use the application in their daily lives during one week. Technical assistance was provided by making contact information available in case of a need in this phase.

Stage 3: Behavioral Observation and Data Collection (Post-Usage Monitoring)
One week after the participants started using the mobile independently, the data about the interactions were gathered, and the specific attention was paid to the security scores that are gained with the help of the point-based motivational system. This enabled the evaluation of behavioral changes of users, especially with regard to their interaction with privacy and permission management functions. The stage data would offer objective sets of the user compliance, system engagement, and possible effects on privacy-conscious behavior.

Stage 4: Post-Usage In-Depth Interviews (Subjective Evaluation and Feedback)
On the end of the independent use interval, structured post-intervention interviews were carried out. These interviews aimed at determining variation in answers to the participants attitudes on the personal data privacy, ease of use as perceived by the participants, satisfaction with system attributes and improvement on the system. Analogy was also carried out by comparing responses of users to those measured during first impression, thereby providing some learning curve and long-term usability.

Data Collection Instruments

The mixed-methods design was used to attain detailed information of participants. This entailed both, standardized quantitative questionnaires and standardized open-ended qualitative interviews.

Quantitative Instruments:

System Usability Scale (SUS):
To determine the usability of the system in a quantitative manner a widely validated 5-point Likert-scale was used and administered as an instrument. The SUS items ranged to include the frequency of intended use, ease of use, complexity, integration of features as well as the ability to learn to use the system.

Ease of Use (EOU) Metrics: Additional Likert-scale questions were composed to also assess specifically important functionalities of the system, such as the intelligibility of permission notifications, the helpfulness of point-based incentive system, and the usability of security dashboard, and easy availability of customization options.

Qualitative Instruments:

Semi-Structured Interview: Open-ended interview questions were organized into six thematic sections to explore the depth and nuance of user experiences:
1. Permission Categorization System
2. Point and Reward System
3. Customization and Settings
4. Learning and Usability
5. Behavioral Changes and Privacy Awareness
6. Overall User Experience and Suggestions

Participants' responses were analyzed using thematic coding techniques to extract recurring patterns, unique insights, and areas for improvement.

Ethical Considerations

All the participants gave informed consent before taking part in the study. The participants were notified of the purpose of the study, the fact that the participation was voluntary, the issue of data privacy, and the fact that they could pull out of the evaluation at any one time without any repercussions. The data that have been collected in the course of the research were anonymized in order to provide these data with confidentiality.

Outcome and Evaluation

The combination of observational data, automatic system-derived usage statistics, standardized usability ratings and qualitative feedback gave a multidimensional assessment of the application. This design of extensive user testing enabled the gradual optimization of the system and confirming its feasibility as a system that will promote privacy enhancing behavior based on the convenience and incentive-based interaction design.

3.2 Summary

This chapter provided a comprehensive and interconnected picture of our research methodology, which included the identification of the vital problem, the collection of user data, the analysis of behavioral patterns, and the development of a customized mobile application. Intermediate testing, which includes device and HCI evaluations, guarantees that only a stable and user-friendly version is presented to actual users for the final evaluation.

Our objective is to create a mobile security system that is not only technically sound but also genuinely usable and relevant to common smartphone users by adhering to this user-centered, multi-step methodology.

Chapter 4

Survey Design

In this chapter, we cover the survey design of our research. Before we started working on building our proposed solution, we wanted to get an idea from our users of what sort of permission related privacy issues they faced on a regular basis. We also wanted to get their opinions on what features might possibly address their issues best. This was done so that we could design our solution to meet their requirements. We have discussed the factors and demographics which helped us to evaluate people's perspectives of app permissions and what measures they employ to safeguard their data. A detailed discussion over our selected demographic has been provided along with descriptions of questionnaire topics, survey methods, statistical analysis and structure of our survey. So, an illustration of the sampling method, survey method and statistical analysis method is described here.

4.1 Demographics

This section establishes the respondent's profile, including age, occupation, gender, region, and smartphone usage. It also evaluates the respondent's willingness to proceed further.

4.1.1 Questions

1. Age range and occupation: Understanding the demographics helps categorize user perspectives based on life stage and professional background. For instance:

- Younger users or students may be more tech-savvy but less aware of app permission risks.
- IT professionals may exhibit higher awareness and carefulness due to professional exposure to cybersecurity concerns.

2. Gender and region: These factors may reveal socio-cultural influences on user behavior, trust levels, and exposure to mobile privacy concerns.

3. Daily smartphone usage: Time spent on smartphones correlates with engagement levels, potentially reflecting the frequency of app interactions and the likelihood of encountering permission-related concerns.

4.2 User Practices and Concerns About App Permissions

This section focuses on the user's current practices and attitudes toward app permissions, their concerns, and their expectations for better security measures.

4.2.1 Questions

1. How often do you check app permissions before installing an app?

- This question assesses users' carefulness in reviewing app permissions, a direct indicator of privacy awareness.

2. Have you ever uninstalled an app due to excessive permissions?

- This reveals whether users take corrective actions when they identify potential privacy threats, showcasing the seriousness of their concerns.

3. Trust in apps on official app stores

- Gauging user trust in platforms like Google Play or the App Store provides insights into whether users equate these platforms with security, influencing their carefulness levels.

4. Concerns about permission misuse

- This question identifies how worried users are about potential privacy violations, emphasizing the need for solutions addressing these concerns.

5. Preferred features for better app security

- This practical question collects data on which features (e.g., instant alerts, detailed breakdowns, educational resources) users believe would help them feel more secure.

6. Primary source for app downloads

- Understanding whether users prefer official stores or third-party websites provides insights into the risk exposure associated with their app acquisition habits.

4.3 Awareness and Engagement with Privacy Tools

This section evaluates users' awareness of privacy tools and their willingness to engage with solutions for improving app security.

4.3.1 Questions

1. Familiarity with app permission control tools

- This question evaluates whether users are aware of tools that allow them to manage app permissions actively, revealing potential knowledge gaps.

2. Motivators for engaging with app privacy

- By presenting options such as instant alerts, reward-based systems, and biometric access, this question gathers insights into what drives users to prioritize their privacy.

3. Interest in apps sending alerts about risky permissions

- Understanding user interest in proactive alert systems assesses the feasibility of solutions that notify users about unauthorized data access or risky permissions.

4. Previous searches for privacy tools

- This question examines whether users actively seek tools to manage their data security, indicating proactive behavior toward privacy concerns.

5. Suggestions for additional data protection measures

- An open-ended question invites users to provide unique ideas and perspectives, uncovering innovative solutions not included in predefined options.

4.4 Survey Implementation

In this section we explained our survey method, question structure and how we conducted the survey in details.

4.4.1 Survey Distribution

As mentioned above, the collection techniques applied to our survey involved online questionnaires in the form of a google form and distributed to different participants through both social media and physically providing them with a QR code. Our data collection targeted anyone who used various smartphone applications in their daily lives to evaluate their understanding of app permissions and the use of any safeguards to protect their sensitive data. We used social media to engage university level students as well as participants who are more tech savvy to ensure that the distribution of our google form was both convenient and widespread. We also forwarded it to our friends and family members. Lastly, we also visited crowded places like corporate offices, bus stands and hospitals to make sure that our participant base included a diversity of different occupations, ages and residential regions as well as people who do use smartphones but are not always accessible through social media platforms.

4.4.2 Survey Question structure

Our survey included 17 questions divided into 3 sections. Apart from the demographics, the other sections had specific questions focused on different perspectives of app permissions and solutions implemented by the participants. These questions are mostly qualitative, mcq type questions with single/multiple selectable answers. However there was also an open ended question that would allow participants to elaborate on what solutions they felt should be implemented.
We classified all of our survey participants into individual classes based on the demographic questions. We then proceed to ask them questions that were vital to our research. Finally we thoroughly analyzed the raw data to be able to examine the obtained responses.

Chapter 5

Survey Results

The chapter provides detailed insights about survey data which examines user behaviors and perceptions alongside their mobile security attitudes. The paper focuses on bringing out the various patterns involving the usage of the applications and the security interests of the different people. These trends will help create better strategies to raise awareness about mobile security.

5.1 Demographic Analysis

To investigate deeper insight into people's thought-process and behavior in the realm of mobile security it is crucial to get to know a little more about our respondents. We surveyed of 363 participants of various ages, employment status, the extent of their smartphone usage, gender and education level. Each of these details is crucial since it reveals how different groups approach the security of their device, trust permissions asking by apps, and the threats they expect.

5.1.1 Age Distribution

In order to investigate the degree of awareness of mobile security we asked participants from all different age groups. Most of the folks who responded were young adults aged 18-24. In fact, out of the 363 people we surveyed, 272 (about 75%) were in this age group, and many of them were university students. Next, we had 58 respondents (16%) aged 25-34, followed by 18 people (5%) aged 35-44, and 10 individuals (3%) who were 45 years or older. The youngest group, under 18, had just 5 respondents (1%).

These results from figure 5.1 show that young adults are the biggest smartphone users and are most concerned about mobile security. However, the small number of older respondents means we need more research to understand how middle-aged and elderly people view mobile security. They might have different security habits due to lower digital literacy or different usage patterns.

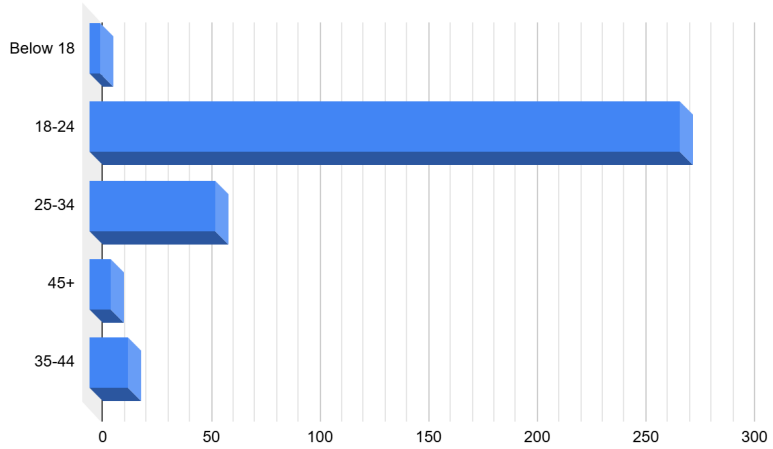


Figure 5.1: Age Distribution of Respondents

5.1.2 Occupation of Respondents

Our survey included people from various professional backgrounds, giving us a look at how different levels of exposure to cybersecurity risks affect their views. We can see from table 5.1 most participants were students, with 287 out of 363 (about 79%) falling into this group. Corporate workers made up 20 respondents (5.5%), followed by 18 teaching professionals (5%), 9 businessmen (2.5%), 8 unemployed individuals (2%), and 6 IT professionals (1.6%). The rest, including laborers, self-employed, drivers, household workers, and others, each represented less than 2% of the total.

Occupation	**Count**
Student	287
Corporate Worker	20
Teaching	18
Businessman	9
Unemployed	8
Labor	7
IT Professional	6
Self-employed	3
Driving	2
Household	2
Others	1

Table 5.1: Occupational Distribution of Respondents

This shows that most of the respondents are still in their early career life hence meets the high percentage of students and fresh graduates found in teaching fields and corporate companies. This implies that they frequently use smartphones for purposes such as education, communication and entertainment and this may determine their perception on app permission and privacy settings. Notably, it is important to understand that the IT professionals in the sample should have a consistently high level of security concern and may be more sensitive to the app permissions and privacy settings.

5.1.3 Smartphone Usage Duration

The time people spend on their smartphones each day from figure 5.2 reveals how much they might be exposed to mobile security risks. The survey shows that the largest group (45.2%) uses their phones for 5-8 hours daily, which means they're highly engaged with apps and online services. Another 27.3% use their phones for 2-4 hours a day, which is considered as moderate usage. Approximately 21.5% spend more than 8 hours on their devices, which indicates a strong reliance on digital technology. Only a small group (6.1%) reported using their phones for less than 2 hours a day.

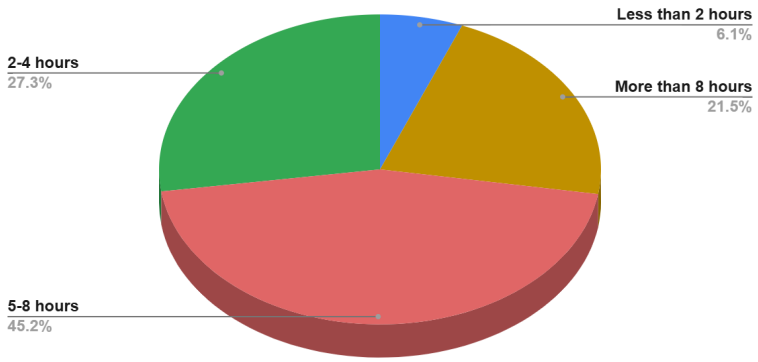


Figure 5.2: Daily Smartphone Usage Among Respondents

These findings show that many respondents are frequent smartphone users, which increases their exposure to mobile security hazards like phishing, malware, and apps asking for unnecessary permissions. Moderate users (2-4 hours) and heavy users (8+ hours) are especially vulnerable because they do more mobile app interaction.

5.1.4 Gender Distribution

The respondents by gender in figure 5.3 revealed that predominantly 70.2% were male while the female formed the remaining 29.8%.

These statistics point to a gender imbalance in the survey, which could affect how we interpret the results on security awareness and behaviors. From previous research it is also revealed that men and women often approach cybersecurity differently. Interestingly, it was observed that men appear to be more self-assured about the security of their devices and their handling of the risks associated with owning and using the devices is much lower than in women, who are less confident in the efficiency of digital technologies. Thus, the studies should attempt to incorporate a better gender distribution to provide a clearer perspective of the disparities. This will be useful in helping us to determine whether or not there is a variation of security awareness and the levels of secure behavior across the different categories.

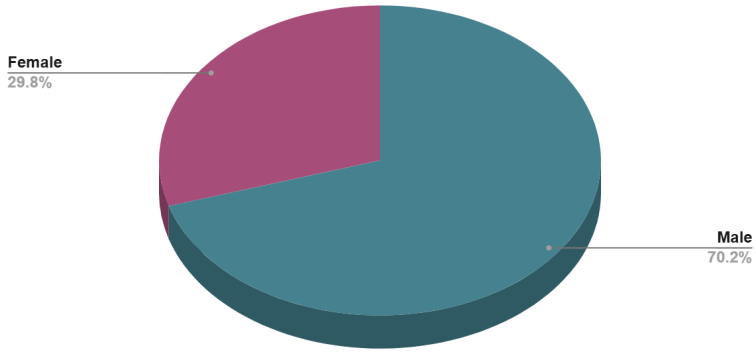


Figure 5.3: Gender Distribution of Respondents

5.1.5 Geographic Distribution

The survey results in figure 5.4 are demonstrating a strong urban bias, with 92.8% of respondents living in urban and 7.2% in rural areas. Such a large number of urban residents can restrain the extent to which we can generalize our findings to a larger population. However, these findings can only offer some insight into urban populations' attitudes and experiences, so further work should be done to examine rural communities' opinions and viewpoints in order to get a clearer picture of this phenomenon.

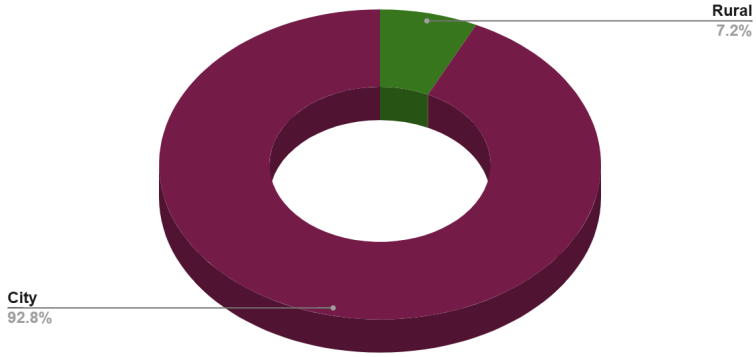


Figure 5.4: Geographic Breakdown of Respondents

5.1.6 Educational Background

From the figure 5.5 Among 363 respondents, 288 respondents were students, which highlights the significant participation of students in the survey. Most of the respondents were 248 (68.32%) undergraduate students. Postgraduate students were 13 (3.58%), followed by high school graduates 11 (3.03%). A small percentage of 13 (3.58%) held doctoral degrees, while 3 (0.83%) fell into the 'primary school' category,

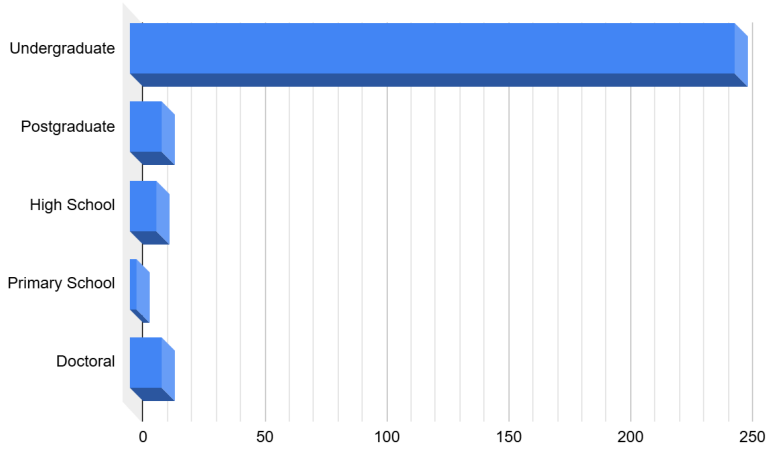


Figure 5.5: Educational Background of Respondents

indicating an alternative educational background. Since a significant percentage of the respondents was the graduate student, which takes 68.32% of the total respondents, thus, it is vital to add the cybersecurity education to the universities. While these students are regular users of the smartphones, many of them may not have had any professional preparatory stint regarding the privacy threats or security sensitization on the mobile platforms. Including this education could really assist them for being safer in the digital world. On the other hand, postgraduate and doctoral level respondents may have a higher propensity towards research-oriented cybersecurity systems, causing them to be more cautious users.

5.1.7 Summary and Implications of Demographic Analysis

Demographic Factor	**Most Common Response (%)**	**Significance**
Age Group	18-24 (74.93%)	Focus on young adult users
Occupation	Students (79.06%)	Importance of educational cybersecurity
Smartphone Usage	5-8 hours (45.2%)	Address security concerns in high usage contexts
Gender	Male (70.2%)	Consider gender-specific security initiatives
Education	Undergraduate (68.32%)	Emphasize university-level cybersecurity education
Geographic Location	Urban (92.8%)	Address potential urban bias and consider rural perspectives

Table 5.2: Summary of Demographic Findings

The results of this study in table 5.2 demonstrate that further research is needed in

order to develop an effective mobile security awareness approach and campaign. To get positive results, interventions need to be targeted following the age, the profession, and use of the smartphone. Moreover, maintaining gender parity and urban bias will lead to narrow down the security system to the whole population. The high proportion of graduating students ensures the important role of the university, so that a culture of cybersecurity awareness is cultivated and students can acquire the knowledge and skills necessary to manage the digital world safely.

5.2 User Perspectives and Carefulness About App Permissions

Assessing user's perception of privacy risks and security threats is significant in analyzing the users' awareness of permissions as related to mobile applications. A number of apps require several permissions thus the chances of compromising people's privacy by collecting unauthorized information or even hacking is evident. This section focuses on the users' behavior towards app permission: how often do they check the permission list before installing an app; do they have more trust in official app store; do they have concerns about misuse of the permissions; what are the preferred security features; and from which source do they prefer to download the apps?

5.2.1 Frequency of Checking App Permissions Before Installation

One of the most basic measurements of mobile security literacy is the frequency with which people review app permission before downloading an app showed in figure 5.6.

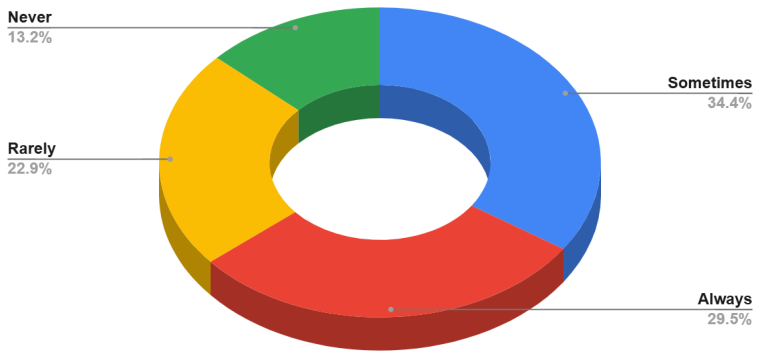


Figure 5.6: Frequency of Checking App Permissions

The results of the survey show that 29.5% of the participants always assess app permissions, therefore, they are conscious about security issues. However, 34.4% of the participants said that they only check permissions at times, which shows that the security practices were moderate and inconsistent. While a 22.9% of users seldom

do so and a 13.2% never check them at all, there is an apparent disregard of mobile security.
These results in table 5.3 highlight the instability in user behavior, where a large portion or altogether neglects permission reviews, or only occasionally checks them. This trend shows that most people do not mind getting convenience at the expense of sacrificing their security to malicious applications or being tracked excessively.

Frequency	**Percentage (%)**	**Security Implication**
Always	29.5	Proactive security behavior
Sometimes	34.4	Inconsistent awareness
Rarely	22.4	Low concern for security risks
Never	13.2	High security vulnerability

Table 5.3: Frequency of Checking App Permissions

These results indicate that, though about one fourth of users are serious about mobile security, a significant number of users are still unaware or indifferent. This underscores the importance of developing awareness programs for people to be willing to check app permissions from time to time.

5.2.2 Denying or Removing Apps Due to Excessive Permissions

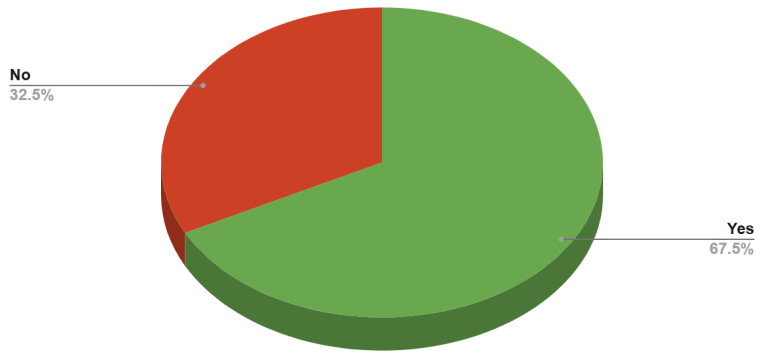


Figure 5.7: Percentage of Users Who Have Denied or Removed an App Due to Permissions

Survey findings in figure 5.7 reveal that 67.5% of the respondents said that they had either deleted or refused to accept the app because of additional permissions; thus, meaning they were now more conscious of the dangers posed by aggressive apps. But only 32.5% of the participants admitted they had never refused or vie an application because of additional permissions, which can be considered as a rather alarming figure regarding their security practices.

67.5% of savvy users probably know about the risks associated with unnecessary access to personal data, such as contacts, location and cameras. However, 32.5% of those who did not participate in this behavior may:
1.Trusted users: Relies on official app stores' permission policies.
2.Unaware users: Do not understand the risks of over permission.
3.Dependent users: Those who ignore the permission policy and install the necessary applications.
The high percentage of app removals due to privacy concerns shows a positive shift in security awareness, though the remaining 32.5% highlights the need to bring transparency to more app permission policies.

5.2.3 Trust in App Permissions on Official App Stores

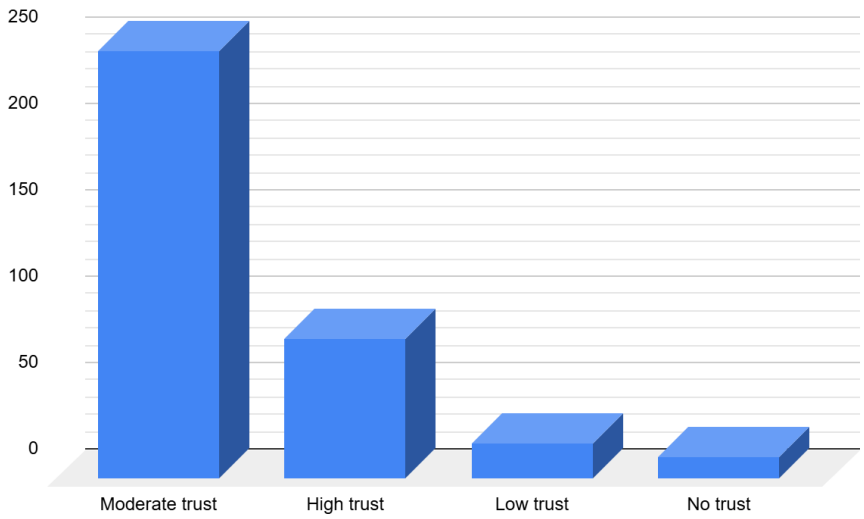


Figure 5.8: Trust in App Permissions on Official Stores

According to the survey results in figure 5.8, 81 (22.3%) respondents showed high trust in apps from official stores such as Google Play Store and Apple App Store. A total of 248 (68.3%) expressed moderate confidence, who think these platforms take security measures, but are somewhat cautious. On the other hand, 21 (5.8%) hardly trust the App Store infrastructure and security measures while 13 (3.6%) completely distrust App Store policies. This creates some doubt as to how safe these app stores are in the first place.
Despite the awareness that Google Play Store and APP Store are genuine sources, there remains a significant number of individuals who are skeptical. This security concern appears to have arisen from past events where malicious apps containing malware made their ways into the App Store. Such an approach might make additional actions like checking app permissions or using additional privacy tools.
Thus, while 34 (9.4%) people claim to have low or no trust at all, it underscores the need for app stores to come clean on their permission requirements and provide better security measures to gain and maintain consumer trust.

5.2.4 Concern About Apps Misusing Permissions

According to the survey results in figure 5.9, the majority of respondents, 183 individuals (50.4%), have expressed some concerns regarding the misuse of app permissions, and 149 individuals (41%) are extremely concerned. Only 31 individuals (8.5%) reported that they are not concerned.

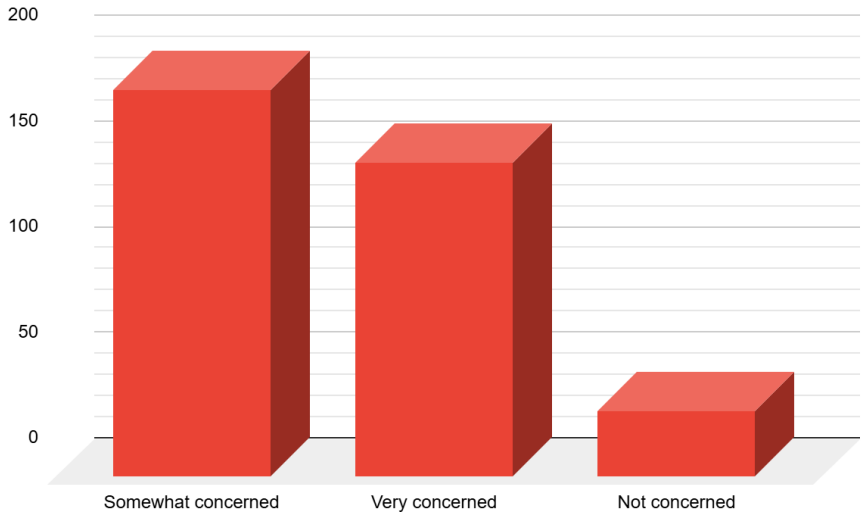


Figure 5.9: Level of Concern About Apps Misusing Permissions

These results indicate that privacy risks associated with app permissions have been widely identified. It is significant to understand that the way 91% of users have voiced their concerns here indicates a heightened recognition of risks that include unauthorized data harvesting, monitoring, and tracking. However, the 31 individuals who are indifferent may either lack awareness or do not trust the existing security measures.

5.2.5 Features That Would Enhance Security Awareness

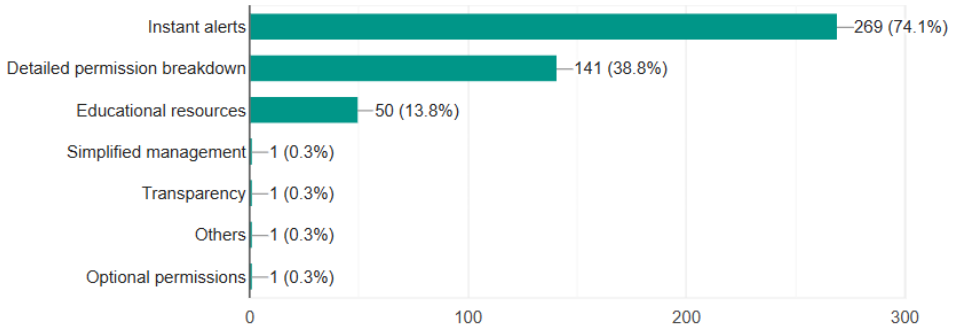


Figure 5.10: Preferred Features for Enhancing App Permission Security

From the figure 5.10 most people (74.1%) said they would like to get alerts right away if an app tries to use something sensitive on their phone. This shows that

people want to be warned in real-time so they can respond right away. Around 38.8% of users also said they like having a detailed list of permission information for each app. This helps them understand clearly what kind of access an app is asking for.

In comparison, only 13.8% thought that learning about security through tutorials or awareness materials would improve their habits. A very small group (0.3%) supported other tools. This shows that people lean more toward tools that are simple to use and do something useful for them right away. They value tools that give alerts and explain permissions, rather than just educational support. Putting together clear alerts with easy-to-read permission info could give users more control and make them feel better about using the app.

5.2.6 Primary Sources for Downloading Applications

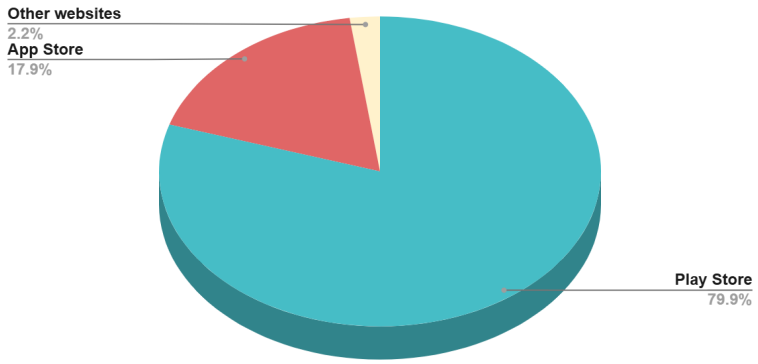


Figure 5.11: Sources of App Downloads

According to Figure 5.11, nearly 80% of people download their apps from the Play Store, 17.9% from the App Store, and only a few—about 2.2%—from other websites.

These numbers tell us that most people trust and rely on official app stores. However, the fact that some users still use third-party websites is a concern, since apps from unknown sources often do not go through proper safety checks.
People may use third-party sites for a few reasons:
1. To get apps that are not available in their region.
2. To access modified or premium features without paying.
3. Because they are unaware of the risks from unverified sources.

This tells us there's a need to inform users more clearly about the dangers of downloading from unsafe places. Helping users understand these risks better might lead them to be more careful when they choose where to get apps.

5.2.7 Summary and Implications of User Perspectives and Carefulness About App Permissions

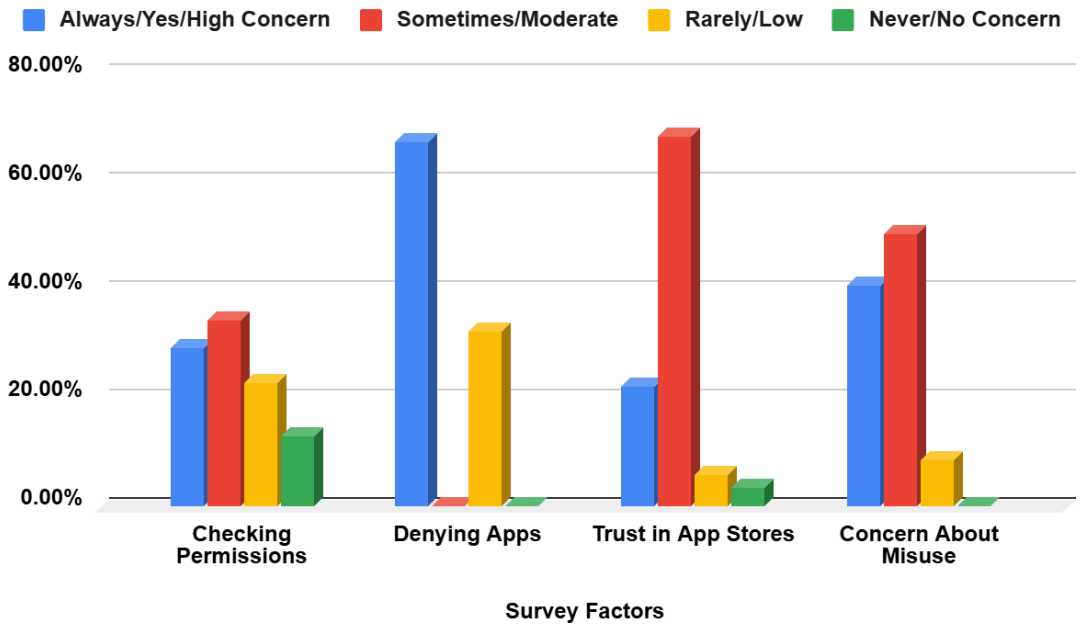


Figure 5.12: User Perspectives on App Permissions and Security Awareness

When we looked at the responses in Figure 5.12, one thing stood out. People said they care about their phone's security, but that does not always show in what they do. Some users said they check what permissions an app asks for before installing it. But many others said they only do this once in a while—or not at all. Some even admitted that they just skip it altogether because they assume apps in the store are already safe.

That kind of thinking reflects a common belief. A lot of users trust that if an app shows up in a popular app store, then someone must have already checked it. So, they go ahead and install it without digging deeper. On the other hand, some users are more cautious—they like to review things themselves. There's a clear difference in how much people rely on store-level checks, and that makes a big impact on how careful they are with permissions.

We also asked if people ever reject permission requests that seem unnecessary. Some said yes—they do. But others admitted they usually just allow everything. One reason could be that they are not sure which permissions are truly risky. Some people are unsure whether blocking a permission will cause issues, so they often allow it just to avoid trouble.

Many people also shared that they feel uneasy about apps trying to access private things—like their contacts, personal photos, or where they are. Many users said that when apps try to access things like photos, contacts, or location, it feels more personal and uncomfortable than other types of access.

So, there is a real gap between how people feel about mobile security and what they actually do. A lot of the time, it is people's everyday habits—not just what they know—that decide how they handle privacy. To help people stay safer, the tools need to support them in everyday use. Things like quick alerts, clear explanations that do not use technical words, or maybe even a simple phone security score could go a long way. With tools like these, even if users are not tech-savvy, they could make better choices about their privacy.

5.3 User's Preference Enhance Privacy and Security

To design better mobile security tools, it is important to know how users think and act when it comes to privacy. This part of our study looks at what users know, how they behave, and what they expect from apps that help protect their data. We gathered users' opinions about permission settings, alerts and their experience with privacy-focused apps. The results help us find ways to build more effective tools.

5.3.1 Awareness of App Permission Control Tools

One of the first things we asked was whether users know about permission settings on their phones. According to the results (Figure 5.13), 68% of users said they knew

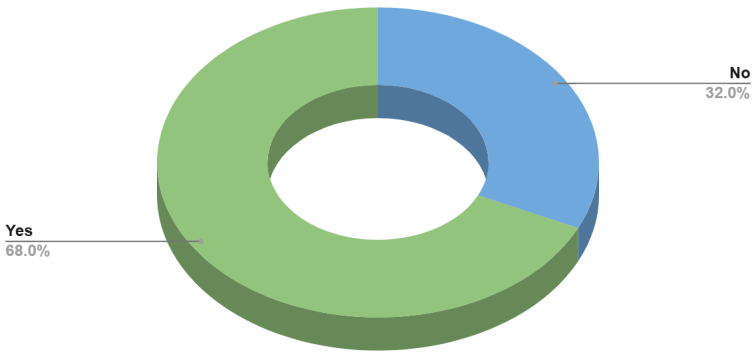


Figure 5.13: Awareness of App Permission Control Tools

about these tools, and 32% said they did not. This shows that while many people are aware, a large group still does not know how to manage app permissions.

Those who understand these settings tend to take action to protect their data. But the ones who do not might give apps more access than necessary without noticing. This highlights the need to make these settings more visible and easier to understand.

5.3.2 Motivations for Engaging with App Privacy

Next, we asked what makes people want to use privacy settings. The top answer (Figure 5.14) was instant alerts, picked by 71.3% of users. People want to be told

right away if an app is using sensitive features like the microphone or camera.
Other things users found helpful:

1. 25.6% of users prefer in-app guides because they show instructions clearly (in the app itself).
2. Around a fourth of people (25.1%) use biometrics such as fingerprint or face ID to authorize activities.
3. Getting points for following good privacy habits was recognized useful by 22.3% of the users.

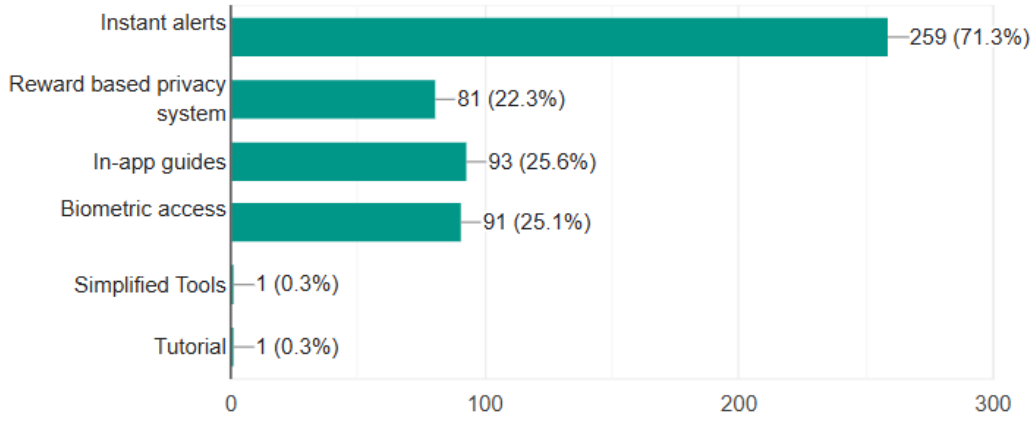


Figure 5.14: Motivations for Engaging with App Privacy

Tools like tutorials (0.3%) or simplified settings (0.3%) were not very useful to most people. Overall, users want privacy tools that give real-time feedback and are easy to understand.

5.3.3 Interest in Security Alert-Based Applications

We also wanted to know if users are open to using apps that give alerts about risky permissions. The results in Figure 5.15 shows:
1. 54.8% said Yes
2. 25.9% said Maybe
3. 19.3% said No

This means over 80% of users are open to trying these kinds of apps. They want more control, especially if the app helps them keep track of which permissions are being used.
Some concerns were shared by people who said No: 1. Too many alerts might feel annoying
2. The app might be hard to use
3. Some do not want another app watching their data

These concerns can be handled by letting users customize how alerts work and making the app interface as simple as possible.

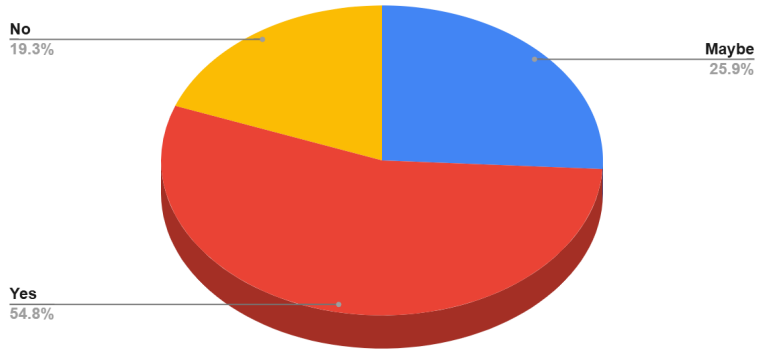


Figure 5.15: Willingness to Use an App That Sends Security Alerts

5.3.4 Searching for Security-Focused Applications

We asked whether users had ever searched for an app to help monitor permissions. As shown in Figure 5.16.

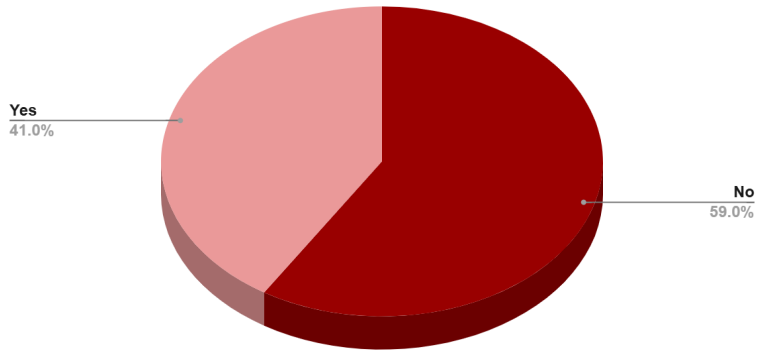


Figure 5.16: Users Who Have Searched for Security-Focused Apps (Pie Chart)

1. 41% had searched for one
2. 59% had not

This shows that most people depend on the default settings in their phone and do not go out looking for extra protection. Those who do search are probably more privacy-conscious. This suggests that awareness efforts could help others start using these tools.

5.3.5 User Suggestions for Improving Mobile Security

Users also gave suggestions on how to make mobile privacy stronger. Here are the most common ones in Table 5.4

Most people wanted instant alerts when sensitive permissions were used. Others

Suggestion	Percentage of Mentions (%)	What It Solves
Instant alert system	31.4%	Letting users know about unexpected access
Clearer app rules	24.2%	Making permission info easier to understand
Blocking extra permissions	20.5%	Stopping apps from asking for too much data
Better data encryption	13.7%	Making private info harder to steal
Tracking app access	10.2%	Helping users see which apps are doing what

Table 5.4: Commonly Suggested Security Improvements

said app policies should be easier to understand and apps should only ask for what they need. Certain users wanted more control over their data security and a way to know how apps are accessing their permission settings.

5.3.6 Summary and Implications of Solutions to Enhance Privacy and Security

Figure 5.17 shows that even though many users know about security tools, only some take the time to use them in daily life. A large group of people knows that tools like permission controls exist, but many still do not use them actively. This shows a common issue: just knowing about a feature does not mean people will actually use it.

A similar trend appeared when users were asked about real-time alerts. Many liked the idea, but fewer were not interested in using it. Most users said they would like to get notifications when an app accesses sensitive information, but not all of them felt strongly about it. Some people are interested and want to stay informed, while others are comfortable with the default settings on their phone. This shows there is a gap between what people say is important and what they actually do in practice. Another thing we found was that many users have not tried to find or install apps that improve security. Instead, they depend on what's already available on their devices. This might mean they trust the system's built-in tools, or it could be that they do not know that other helpful apps exist. This tells us that some people simply trust their phones to handle security and do not take any extra steps themselves.

Overall, this points to a common privacy issue. Although most people believe phone security is necessary, it does not always result in them acting on it. While some users are more active and take time to manage their settings, others think the phone's default tools are good enough. To change how users act, making users aware of the dangers is not always enough. There needs to be a system that also encourages and motivates users to take action. Without this kind of support, many users may

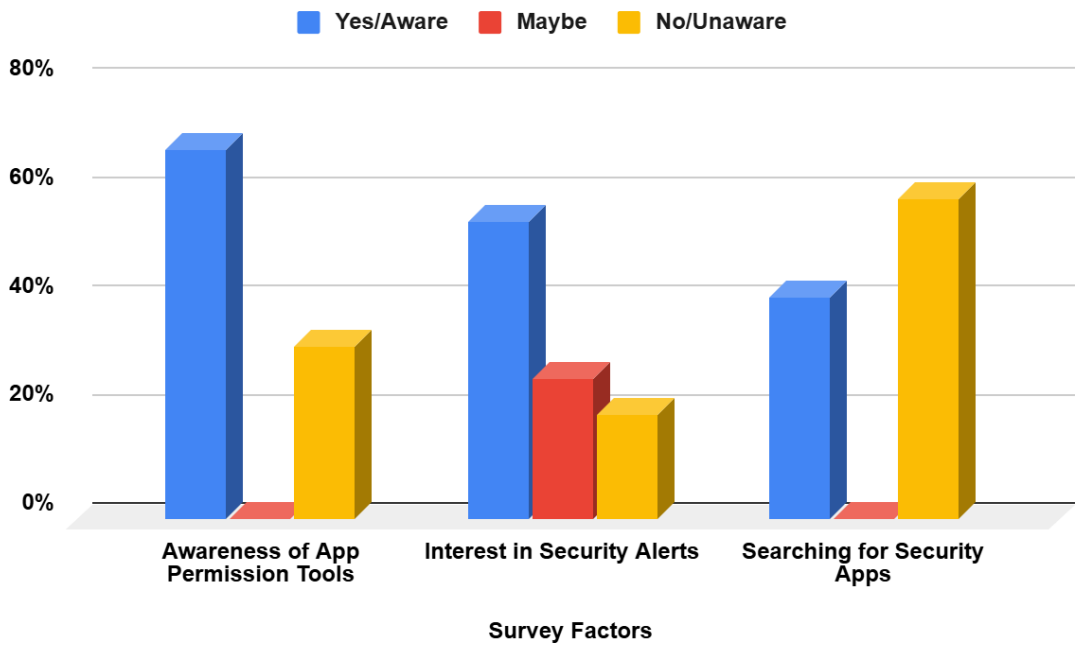


Figure 5.17: User Awareness & Security Preferences

continue using their phones without realizing they are still at risk.

5.4 Survey Results Discussion

This chapter looked at how people really think and behave when it comes to mobile app security. Something that really stood out from the answers we got is this: even when people know that mobile security matters, they do not always act on it. About one out of every three participants said they usually check app permissions before installing something. But many others admitted they only do it now and then, and some said they never check at all—roughly 13% of the group. There's still a clear difference between being aware of privacy issues and actually doing something about them in daily life.

What we found was quite telling—about 67.5% of users said they had either denied permissions or removed apps completely because of privacy concerns. This shows that more people are becoming aware and careful about mobile security. Still, more than 30% of users tend to accept app permissions without much thought. This represents a great need for more straightforward tools with better support to help people make smart and confident decisions about their privacy. Even though most people prefer downloading apps from official stores, a large number still worry that some of these apps might misuse their access. At the same time, more than 91% said they're at least somewhat worried about how apps use their personal data—which makes that gap between concern and action even more important to address.

User's responses were surprisingly consistent, when we asked them what would make them feel more secure. The majority—about 74%—wanted instant alerts whenever

apps try to access sensitive information. A simple and easy-to-manage approach to control app permissions has been preferred by some users. Fewer were interested in reading or learning through educational content—most want tools that work in the background and help automatically, without extra effort. Interestingly, though 68% of users were aware about phone's permission settings, only 41% had actually tried to find an app to manage them. This tells that knowing something exists does not always lead to action. A small push like clear benefits or gentle reminders is often needed by people—to move from awareness to actually doing something about it.

In short, users value privacy, but they need apps that are simple, informative, and proactive. To stay conscious instead of feeling overwhelmed—features like instant alerts, straightforward dashboards and automatic permission checking may help users. Such tools quietly support safer habits to enable safer habits and practices so that individuals can manage their privacy without being technologically inclined.

Chapter 6

TRACKO: a Privacy Preserving Monitoring Mobile App Solution

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 [59]. 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.

6.1 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 be 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. It 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. Figure 6.1 shows our system block diagram.

6.1.1 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

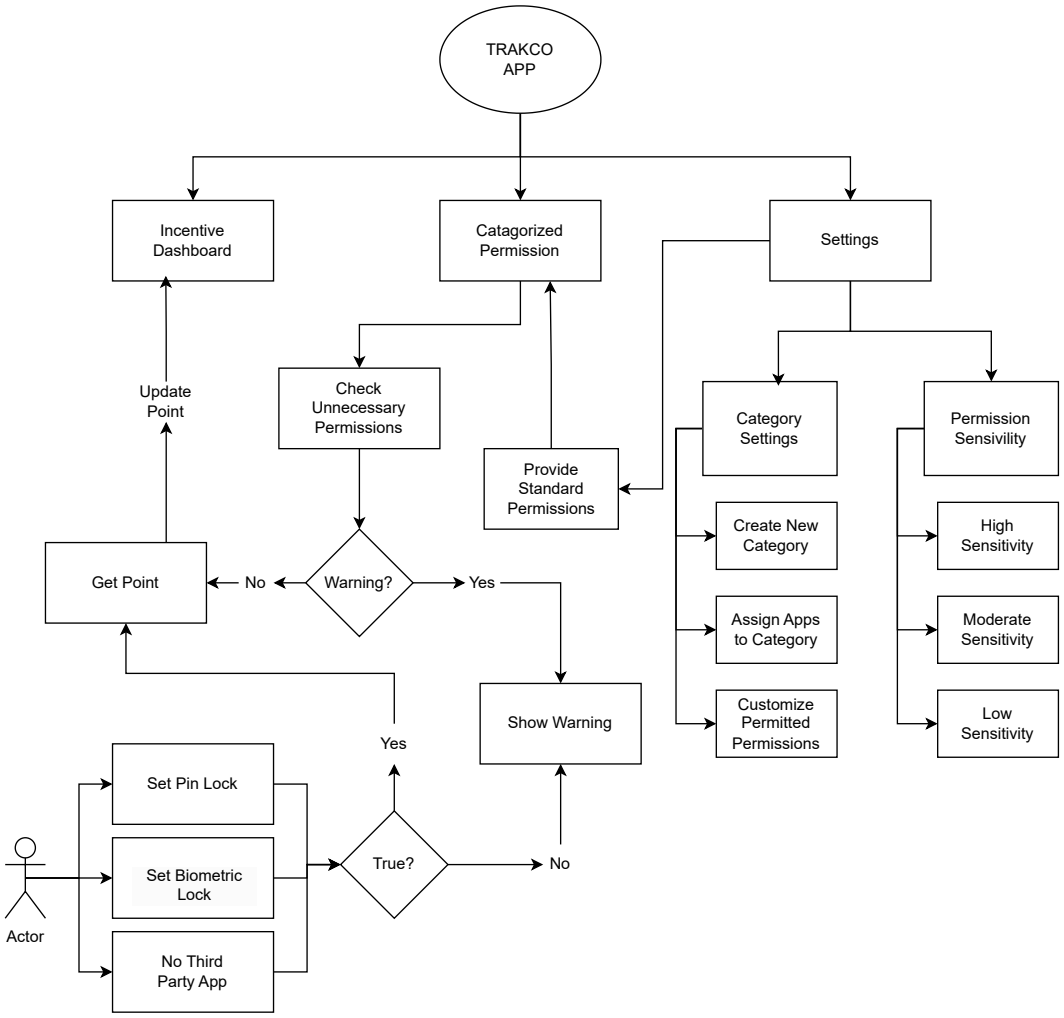


Figure 6.1: System Flow Diagram

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:

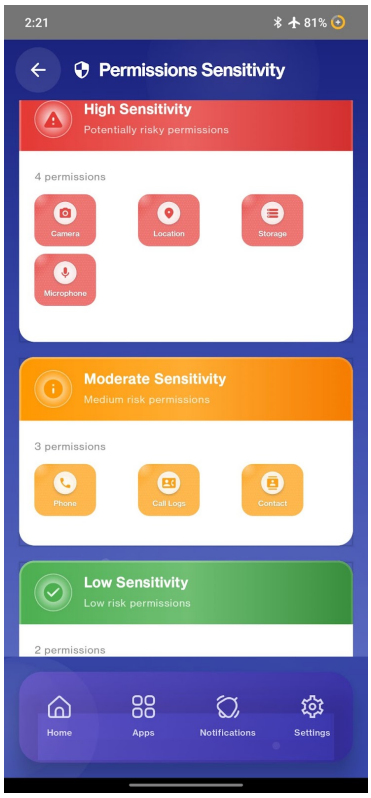
1. Phone Password: This segment ensures whether you have given a password for your phone or not. According to a 2018 Kaspersky Lab study, more than half of people don not password-protect their mobile devices. The system provides 20 points to the user for using passwords to protect their phone. Usually, 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 sys-

tems 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 does not 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. For ensuring 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:
High - allotted 60 points and has direct live tracking threats.
Moderate - allotted 30 points and has indirect tracking threats.
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.



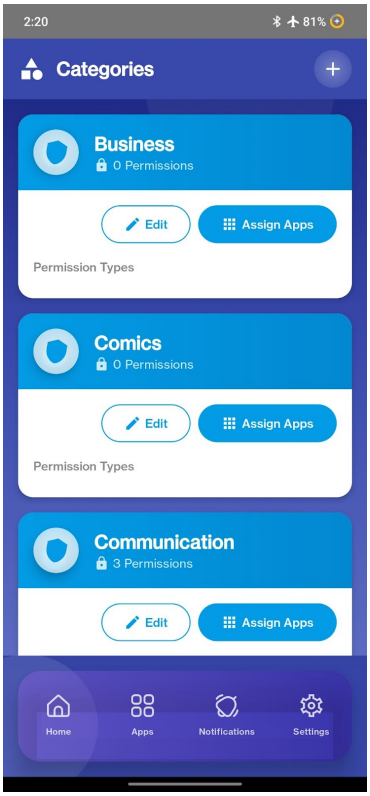
6.1.2 Categorized Permission

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 are 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 the user can specially categorize any app of their preference and customize the permissions required for that particular app in question.
Our suggested given categories are :

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.



2. Video players and editors: These segment includes apps that are used for photoshopping or editing the pictures or videos.

Allocated Permissions: camera, microphone, gallery

Examples: CapCut, Filmora etc.

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

Allocated Permissions: location

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

4. Tools and Utilities : This segment includes apps that can be used as operating softwares and VPN's.

Allocated Permissions:

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

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

Allocated Permissions:

Examples: Cricbuzz, Cricket Line Guru etc.

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

Allocated Permissions: gallery, files

Examples: TikTok, Instagram,Facebook, Reddit etc.

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

Allocated Permissions:

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

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

Allocated Permissions: files, gallery

Examples: CamScanner, Chatbot, Microsoft etc.

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

Allocated permissions:

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

10. Maps and navigation: includes all the navigation related apps.

Allocated Permissions: location
Examples: Pathau, Uber, JoyRide etc.

11. Medical : Includes all the medical service apps.
Allocated Permissions:
Examples: Shukhee, MedEx, DocTime etc.

12. Libraries and demo(Ebooks) : Includes all kinds of online reading apps.
Allocated Permissions: files
Examples: Holy Quran, Holy Bible etc.

13. House and home (Alexa , google home) : Includes home assistance apps.
Allocated Permissions: microphone
Examples: Home Security Camera, HelloTask etc.

14. Health and fitness: Includes fitness and health related apps.
Allocated Permissions: Bluetooth
Examples: MyFitnessPal, Calorie Counter, Step Tracker etc.

15. Games: All kinds of actions, strategic, online, offline, adventure games are included.
Allocated Permissions:
Examples: Mobile Legends, Candy Crush, Angry Birds etc.

16. Food and drink : Includes food delivery, food review apps.
Allocated Permissions: location
Examples: Foodpanda, Food, Uber Eats, Zomato etc.

17. 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.

18. Entertainment : All forms of entertainment apps are included in this segment.
Allocated Permissions:
Examples: Sony LIV, Netflix, Toffee, Bongo, Amazon Prime etc.

19. Education : This segment includes online education platforms, academics helping apps etc.
Allocated Permissions:
Examples: Phootomath, 10 Minutes School, Duolingo, Khan Academy etc.

20. Dating : Includes all sorts of online dating or relation forming apps.
Allocated Permissions: gallery, location

Examples: Tinder, Bumble, Flirtify etc.

21. Communication : Includes all types of online communications apps.
Allocated Permissions: microphone, camera, gallery, files
Examples: Imo, Messenger, WeChat, Skype, Whatsapp Business, Viber etc.

22. Comics: Includes apps that are ususally manga or comics etc.
Allocated Permissions:
Examples: MangaHub, WebToon, Tapas, Wattpad etc.

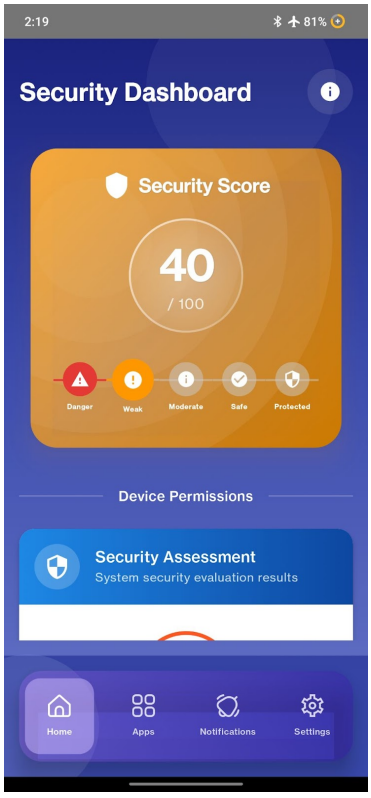
23. Business : All kinds of business affiliated tools and apps are included in this segment.

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

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

6.1.3 Scoring assessment

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



Danger: 0-30
Weak: 30-50
Moderate: 50-70
Safe: 70-90
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.

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:
High - allotted 60 points and has direct live tracking threats
Moderate - allotted 30 points and has indirect tracking threats
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. For a better understanding of the point assessment, the following table 6.1 is given:

High-60 points	**Moderate-30 points**	**Low-10 points**
Microphone-15 Camera-15 Storage-15 Location-15	Phone-10 Contact-10 Call log-10	Nearby devices-5 Calendar-5

Table 6.1: Permission points classification table.

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:

In every column of the table, the total points are fixed as long as there is at least one element present in that column.

If a column in the table 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.

For each column of the 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.

After the total points from each column are added, the numbers are converted from 100% to 40%.

6.2 Development Process

The creation of privacy preserving monitoring system is done using the kotlin and java has 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.

6.2.1 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 actually would 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.

6.2.2 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 included 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 analyses 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. 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.

6.3 App Limitations

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 does not allow the application to be notified of the change of password in a week. As the application is not 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 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, internet. Although many functions can be seen, our application only focuses on these 4 functions, we expect broaden our horizon in future.

Chapter 7

Evaluation via User Study

Effective user testing and feedback is critical in the development and refinement of mobile applications, particularly for tools related to privacy and device security. This section outlines the methodology and techniques employed to evaluate a standalone Android APK designed to enable users to view, manage, and modify the permissions granted to other applications on their device.

7.1 Study Design

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

7.2 Interview Design

The questionnaire consists of the user's personal information, several questions divided into types, such as
Quantitative - System Usability Scale(SUS), Ease of Use(EOU)
Qualitative - Permission Categorization System, Point and Reward System, Ease and Learnability, Behavior 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 behavior
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:

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

B. Point and 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)?

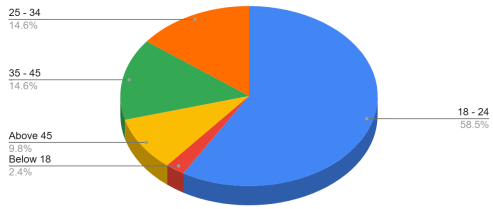
D. Learning and Usability:
1. Did you need a tutorial to understand how the app works?
2. Which part was the hardest to understand?
3. How can you make this app easier to use for you?

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?

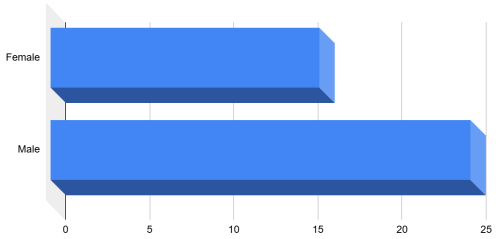
F. Overall Experience:
1. Which feature did you like the most and why?
2. Which part of the app needs improvement in your opinion?
3. Would you suggest this app to others? Why or why not ?

7.3 Participant Demographics and Usage

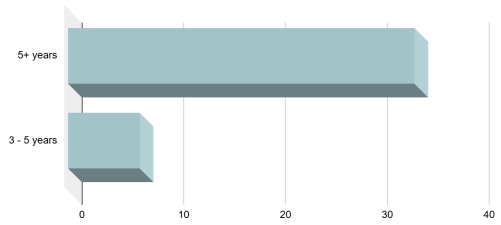
The research included 41 people selected from the intended user demographic. The majority of participants were young adults, with approximately 58.5% aged 18–24 and the subsequent largest group (14.6%) aged 35–45 (Figure 7.1a). The remaining individuals were aged 25 to 34 or over 45, with only one member under 18. A minor male majority was observed (25 males compared to 16 females)(Figure 7.1b). The participants' occupational backgrounds were diverse: around two-thirds were undergraduate students, while others were graduate students, professionals (such as bankers, software engineers, government servants), and homemakers. All participants were proficient smartphone users, with 34 having utilized a smartphone for over five years (Figure 7.1c). Daily mobile Internet usage was significant, with over 70% of individuals indicating they utilized mobile data for three or more hours each day (Figure 7.1d. These statistics indicate that our users were proficient and consistently active online.
Prior to using our application, the majority of participants rarely reviewed app permissions. From figure 7.2a almost 14.6% reported that they consistently evaluated



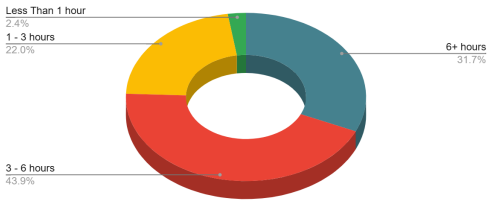
(a) Age Distribution of Participants



(b) Gender Distribution of Participants



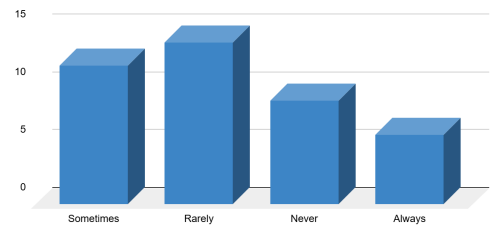
(c) Smartphone experience of Participants



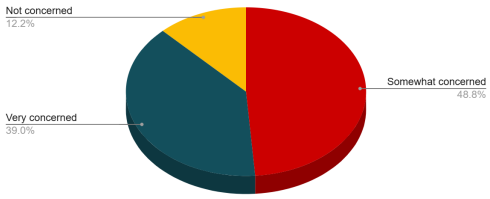
(d) Internet Usage Per Day of Participants

Figure 7.1: Demographic Insight

permissions; nearly two-thirds (about 26 out of 41) indicated that they did so only "sometimes" or "rarely." The majority expressed apprehension regarding their mobile privacy, with most categorizing their fear as "somewhat" or "very" significant (Figure 7.2b. This indicates a disparity between user awareness and actual behavior. Participants valued privacy yet did not consistently regulate permissions. The demographics suggests a user base that is technologically proficient and conscious of privacy, but does not routinely verify permissions. This profile indicates that an app aimed at enhancing permission awareness was fulfilling a genuine necessity.



(a) App Permissions Review by Participants



(b) Participants Concerns about Mobile Privacy

Figure 7.2: Participant's Initial Awareness

7.4 First Impression on App

7.4.1 Qualitative Feedback

This part of the research was executed at the initial stage of user engagement with the mobile security application. Participants were requested to convey their initial

impressions immediately following the exploration of the app for the first time from our sample device. These impressions were gathered before to any formal testing, enabling us to obtain unprompted reactions unaffected by comprehensive usage or interview protocols. The replies in (Figure 7.3) indicate unrefined expectations, initial surprises, and instinctive reactions to the design and features.

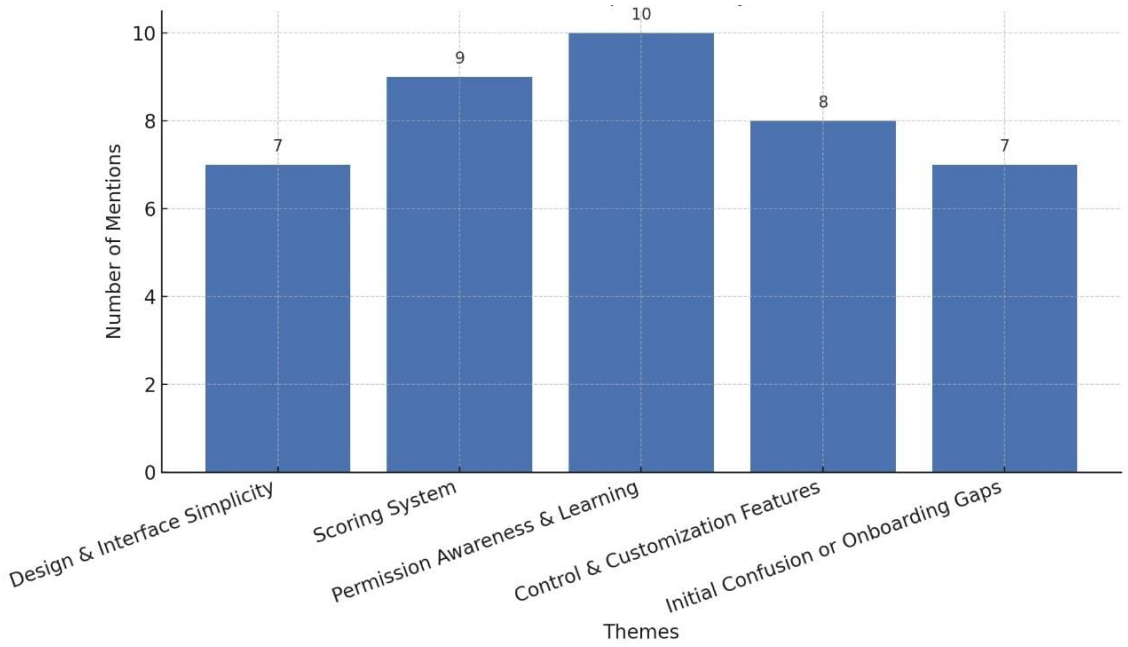


Figure 7.3: First Impressions of Users on App

Initial impressions revealed five predominant themes:

1. Design and Interface Simplicity

A multitude of users commended the application's smooth and intuitive design. They defined it as "simple and clean" and emphasized that the "UI design must be fun to use". Some expressed pleasure at the clarity of the permission notifications, remarking that they "did not expect the permission alerts to be this clear". This suggests that the visual and interface design facilitated comprehension of privacy-related functions.

2. Scoring System

The point-based scoring system was notably distinguished among users. Several indicated that the scoring method instilled a sense of accomplishment about their phone and that it did not resemble a boring security instrument, but rather felt like advancement. One user likened it to "playing a game," illustrating how a point-based reward system enhanced user engagement by making it more interesting and encouraging.

3. Permission Awareness and Learning

A significant number of users demonstrated astonishment or newfound awareness over their data privacy. One individual said, "I never knew my phone was sharing so much information" while another remarked, "Some games and shopping apps were using my GPS makes you wonder how private your data really is." This indicates that the app functioned not merely as a tool, but also as an educational

experience.

4. Control and Customization Features
Users emphasized the significance of self-managing permissions. The drag-and-drop sensitivity setting was characterized as "enjoyable" and others valued the ability to "control everything from one place". Despite the occasional acknowledgment of the laborious nature of manual categorization, one user appreciated the autonomy it provided, stating, "I have to categorize the apps on my own, which gives me more control".

5. Initial Confusions or On-boarding Gaps
Although numerous users adapted swiftly, several expressed initial confusions. Feedback included "looked like something to do with app permission but could not understand how it works", while others did not immediately comprehend the point system or customization features. This underscores the necessity for enhanced onboarding or tutorials in subsequent iterations.

The initial impressions facilitated our comprehension of users' emotional and cognitive responses to the app prior to formal testing. Favorable responses to the design, scoring system, and permission control aspects indicated initial involvement, however the sporadic instances of misunderstanding highlighted areas for further enhancement in guidance. These insights informed subsequent phases of user testing, establishing a robust basis for assessing more profound usability and behavioral transformations over time.

7.4.2 Quantitative Feedback: App Security Score Progression (Score at Installation vs. Score One Week after Installation)

To assess user involvement and alterations in security behavior over time, we compared users' security scores after their initial app interaction with scores obtained after one week of usage. This segment of the study involved 41 participants.

Initially, users received scores ranging from 20 to 60, with a mean score of 40. The initial scores indicate a fundamental comprehension of phone security, since users engaged with the application with minimal assistance. Following one week of consistent usage and engagement with app functionalities such as sensitivity categorization, permission notifications, and the point-based reward system, the scores markedly enhanced. After one week, the maximum score attained was 78, while the average score rose to 67.65 (Figure 7.4).

The majority of users demonstrated significant advancement, with the most substantial individual enhancement being a 50-point increase. Nonetheless, two individuals encountered a minor decline in their scores (from 59 to 55 and 47 to 45), potentially attributable to the removal of security elements or the neglect of notifications. These exceptions underscore the significance of sustained engagement for optimal outcomes.

The average improvements among all participants was 27.65 points, signifying that the application effectively encouraged users to embrace safer mobile practices (Fig-

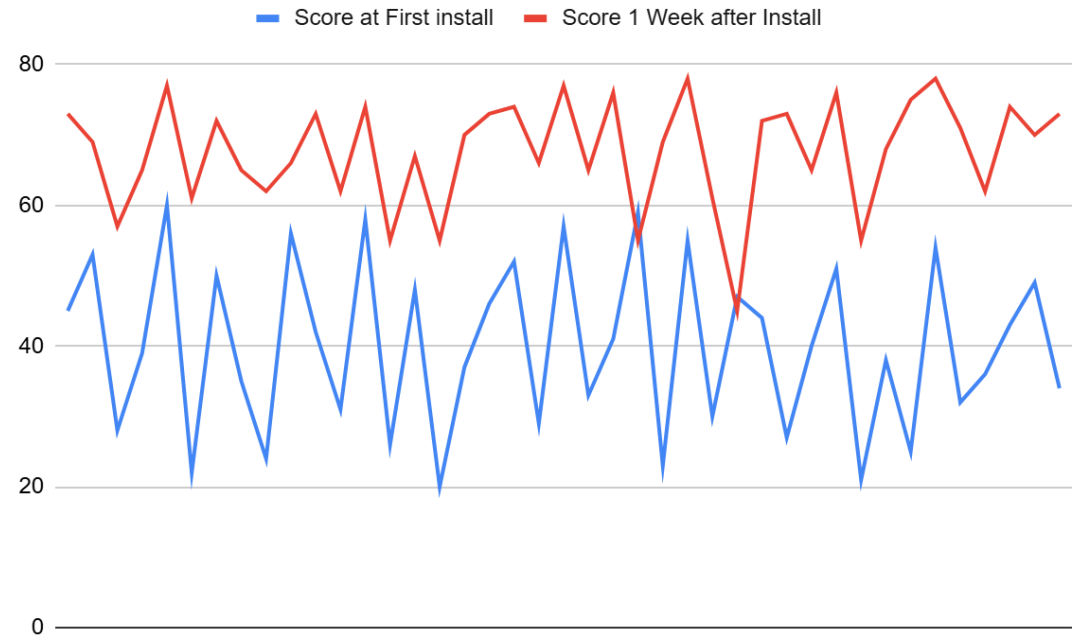


Figure 7.4: Participant's Score at First Install vs. 1 Week after Install

ure 7.5). This quantitative trend corresponds with the app's design principles, which emphasize awareness, motivation through scoring, and incremental behavioral modification. The results confirm the efficacy of the app's interactive security features in improving user privacy awareness and proactive conduct.

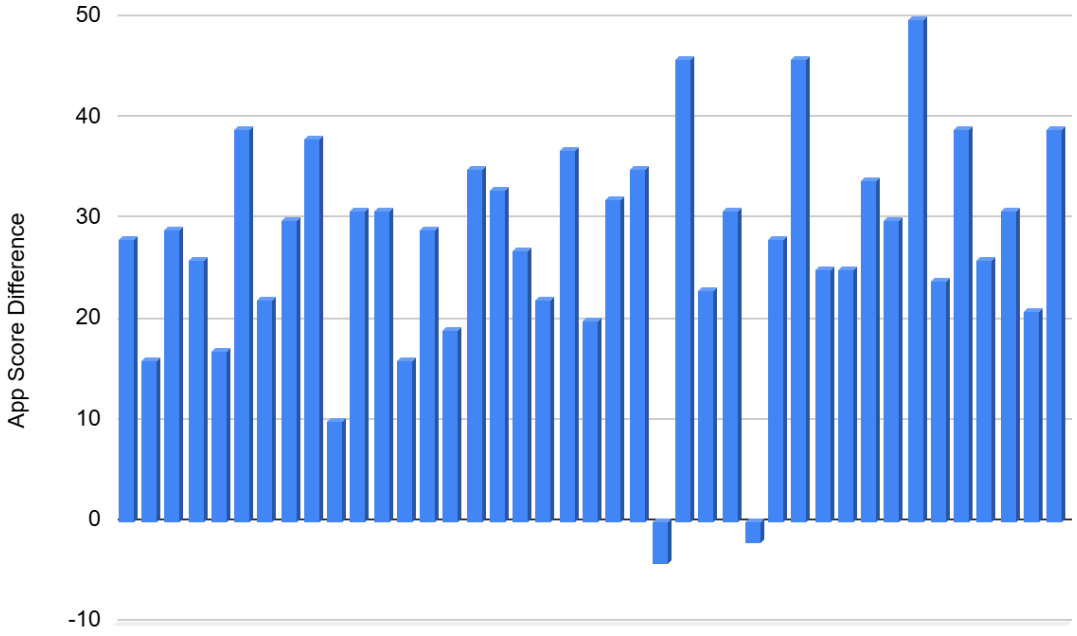


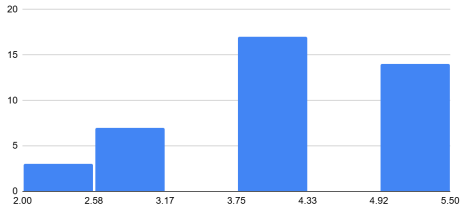
Figure 7.5: Users' App Score Difference

7.5 Interview Findings

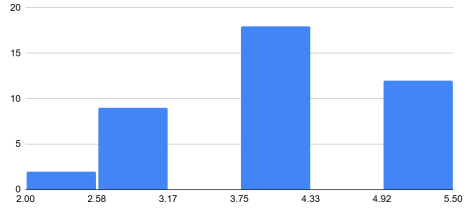
7.5.1 Quantitative Feedbacks

System Usability (SUS) Results

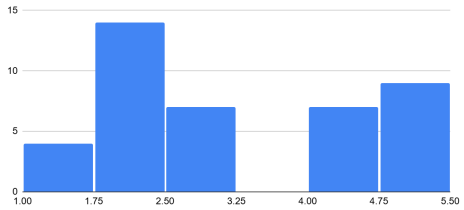
Participants evaluated five SUS statements (rated 1 = strongly disagree to 5 = strongly agree) addressing general usage intention, usability, necessity for assistance, feature organization, and learning requirements. The outcomes were exceedingly favorable. From figure 7.6a Approximately 75% of users concurred or strongly concurred that they would utilize the app regularly (mean = 4.02 out of 5), and a comparable percentage found it user-friendly (mean = 3.97 out of 5). The majority of participants perceived the app's features as well-organized (mean = 4 out of 5). Approximately one-third concurred that assistance would be necessary (mean = 3.07 out of 5), indicating that the overwhelming majority felt assured in their ability to navigate the app autonomously (Figure 7.6b). For instance, following the instruction, one participant remarked, "I can use this app easily" underscoring that even new users could swiftly use this app without difficulty.



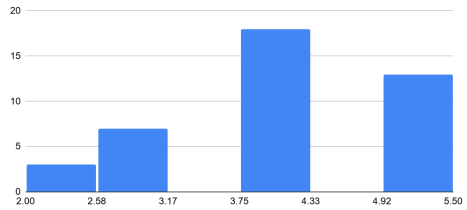
(a) Users' Willingness to Regularly Use the App



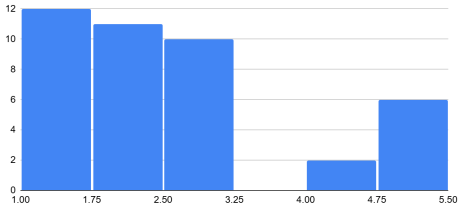
(b) Perceived Ease of Use of the App



(c) Perceived Need for Assistance While Using the App



(d) Perception of Feature Arrangement



(e) Learning Effort Required Before Using the App

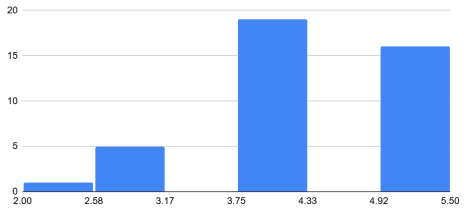
Figure 7.6: System Usability Findings

Based on these SUS data, it looks like the app is generally easy to use and meets users' needs. Participants perceived the interface as intuitive and user-friendly, necessitating minimal training, as indicated by their consistently favorable evaluations(Figure 7.6c, 7.6d, 7.6e).

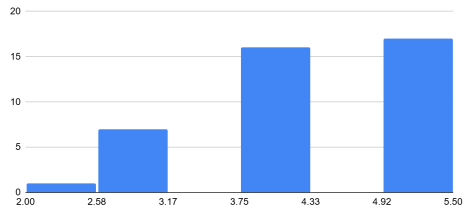
Ease of Use Results

Additionally, using a 1–5 agreement scale, participants evaluated each feature for clarity and usefulness. The statements addressed the security dashboard, the customization settings, the points-and-rewards system, the permission notifications, and the explanation of necessary permissions. There was a uniformly excellent grade. For instance, approximately 80% of participants concurred that the permission alerts were easily comprehensible (mean= 4.22 out of 5), and a comparable percentage stated that the application assisted them in determining which permissions were genuinely essential (mean= 4.19 out of 5). The points system was also found to be encouraging for secure behavior by approximately 80% of respondents (mean= 4.15 out of 5). The majority of respondents (85%) expressed satisfaction with the security dashboard's ability to maintain awareness of their phone's security (mean= 4.27 out of 5). Additionally, approximately 75% perceived the customization settings as user-friendly (mean= 4.05 out of 5)(Figure 7.7a, 7.7b, 7.7c, 7.7d).

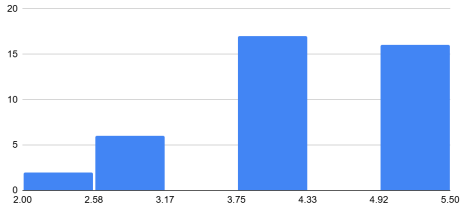
.



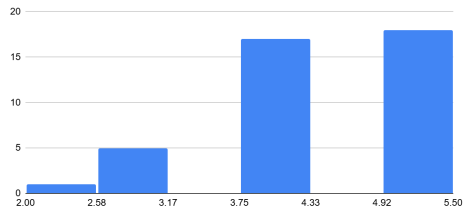
(a) Clarity of Permission Alerts with App Support



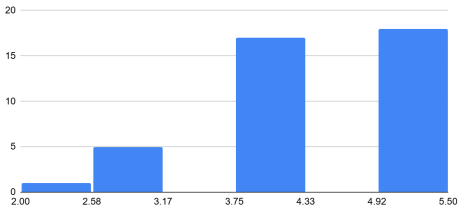
(b) Understanding Permission Necessity



(c) Motivation to Maintain Safe Behavior from the Point System



(d) Awareness Raised Through the Security Dashboard



(e) Ease of Using Customization Settings

Figure 7.7: Ease of Use Findings

The constantly high ratings suggest that every principal element of the app was regarded as lucid, informative, and beneficial (Figure 7.7e). The quantitative findings indicate that participants perceived the app's primary features as intuitive and beneficial.

7.5.2 Qualitative Feedback

In addition to surveys, we performed structured interviews to gather open-ended input. The qualitative questions were categorized thematically in relation to the app's functionalities. We highlight the key findings for each theme below, accompanied by participants' comments.

Permission Categorization

The permission alert function prominently emerged as one of the most significant elements of the application. The objective was clear: to alert users when an application requests sensitive or ostensibly superfluous rights. For many, this was their initial realization of the extent to which their applications were accessing data without explicit justification. When asked about their preferences, users predominantly

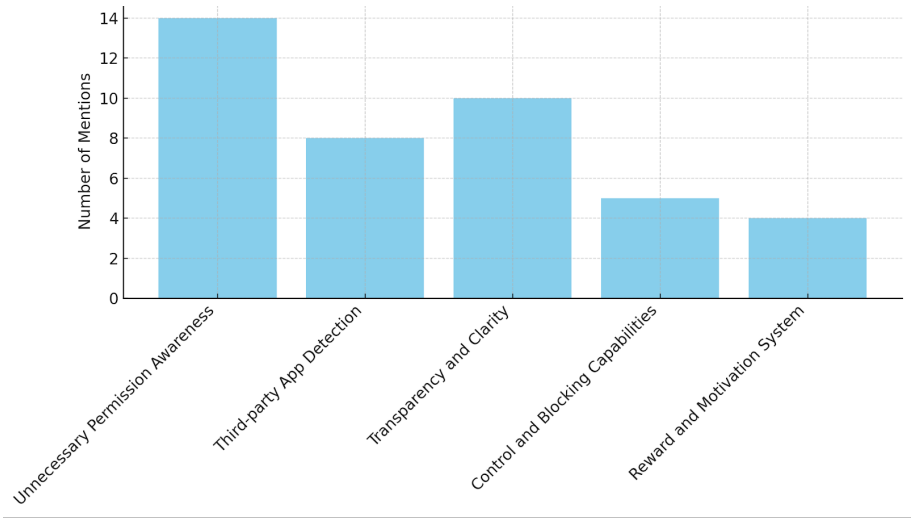


Figure 7.8: Users' Favorite Aspects of the Permission Alert Feature

preferred the Unnecessary Permission Awareness. Fourteen participants indicated that notifications prompted them to recognize that applications, such as calculators or photo editors, were requesting unnecessary access (Figure 7.8). One user stated, "Helped me understand the unnecessary permission on my phone and app-related security". Another said, "Unnecessary permission tracking which was unknown before". Numerous users appreciated the Third-party App Detection feature, with eight individuals highlighting its capability to notify them about software not obtained from reputable sources: "In case of third -party apps it alerted me and unnecessary permissions could be removed", stated one user. Transparency and clarity emerged as a prominent topic, with eleven participants commending the system's explicit presentation of "exactly what permissions each app wanted and why", including some that were sensitive. Simultaneously, five users appreciated the capacity for prompt intervention via Control and Blocking, including the options to revoke access or remove the application, "I could block any unwanted permission by my own" remarked one participant. Finally, several individuals saw that Motivation Through Rewards associated with warnings rendered privacy checks more interesting, with one characterizing it as "a reward system that incentivizes users to interact with the app."

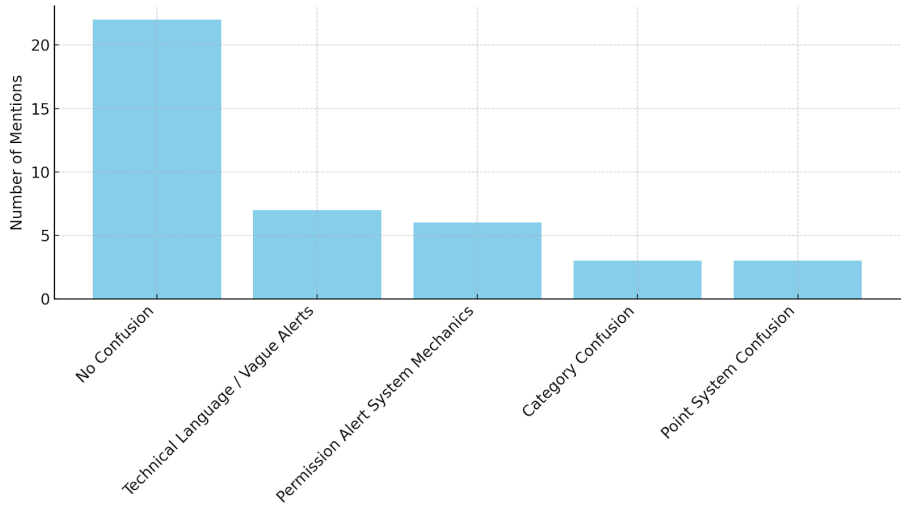


Figure 7.9: User Confusions or Misunderstandings Regarding Permission Alerts

From figure 7.9, regarding uncertainty, the majority of users (22) indicated that the system was straightforward and intuitive. Seven participants reported concerns over Technical Language or Vague Alerts, with one stating, "Some messages were too technical for me". Six other individuals expressed uncertainty over the correlation between the Alert and Points system, stating, "I could not understand how to increase the points at first". Three individuals expressed Category Sensitivity Confusion, although they said that prolonged usage enhanced their comprehension.

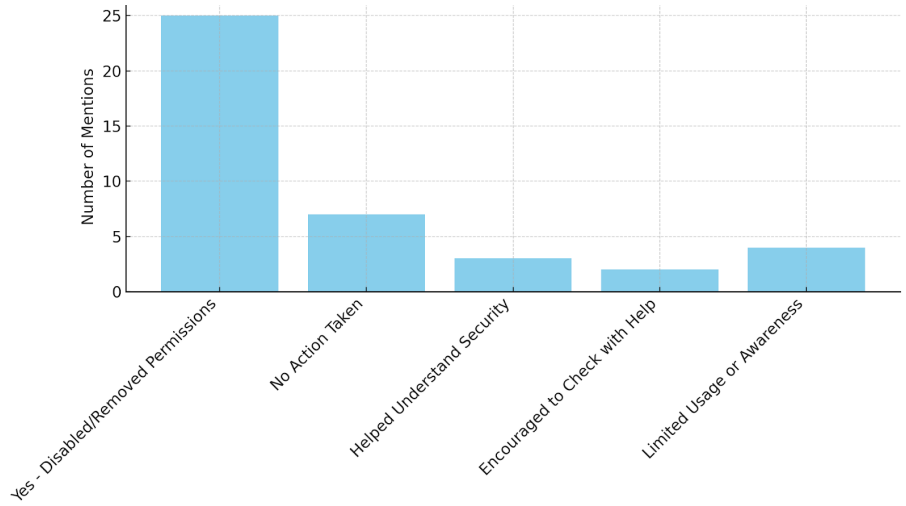


Figure 7.10: User Actions Taken Based on Permission Alerts

The most persuasive indicator of effectiveness was the number of participants (25) who acted upon the warnings (Figure 7.10). Users reported revoking permissions, such as camera or location access—"I removed the camera permission from Bkash", stated one or deleting applications like CamScanner upon receiving alerts regarding dubious access. Four individuals became more aware but had not yet taken action, while two sought assistance from family members, "I asked my son to help turn off camera access on a news app". A limited proportion (7) identified Restricted Utilization as the rationale for their inaction thus far.

In conclusion, permission alerts not only provided information but also altered behavior. Users demonstrated enhanced control over their digital privacy, ranging from restricting permissions to deleting applications. With minor enhancements to simplify language and clarify the relationship between warnings and rewards, this feature could significantly improve its effectiveness in fostering privacy behaviors.

Point and Reward System

The point and reward system in our mobile security application was developed to promote safe digital practices by converting positive behaviors into measurable advancement. The majority of participants deemed this feature captivating and inspiring, with numerous individuals articulating its influence on their comprehension of mobile security.

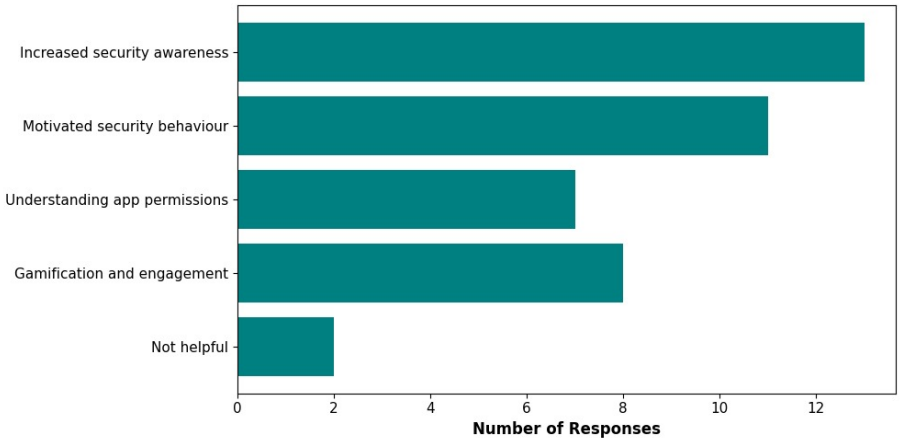


Figure 7.11: User Perceived Helpfulness of the Point System

The benifits mentioned was its contribution to enhancing awareness regarding privacy and security. A user remarked, “It helped me understand my phone’s security level”. Some said it inspired them to “become more alert about permission access” or “remove suspicious permissions”. From figure 7.11 a significant cohort (13 out of 39) reported increased awareness regarding their phone’s security, while 11 individuals indicated that it directly motivated them to undertake privacy-oriented measures. Many users valued the point based reward system of the experience, with one remarking, “Felt like game progress,” so emphasizing that security duties became more pleasurable.

The study into user motivation produced largely positive outcomes. Approximately 21 interviewees explicitly affirmed their agreement, whilst 9 expressed moderate motivation (Figure 7.12). Numerous individuals likened compared it to a game in which “earning points felt rewarding” and “made me want to improve my habits”. One said, “It made good habits measurable”, while another concurred, “Yes! Felt like a game”. Some expressed uncertainty regarding the long-term implications; yet, the point system generally yielded a favorable behavioral outcome.

The situation here was rather more varied. The majority (22 of 43) indicated that they encountered no confusion (Figure 7.13). Nevertheless, seven participants deemed the point allocation ambiguous, such as, certain acts awarded 10 points, while others conferred 40, lacking a discernible justification. One remarked, “I did

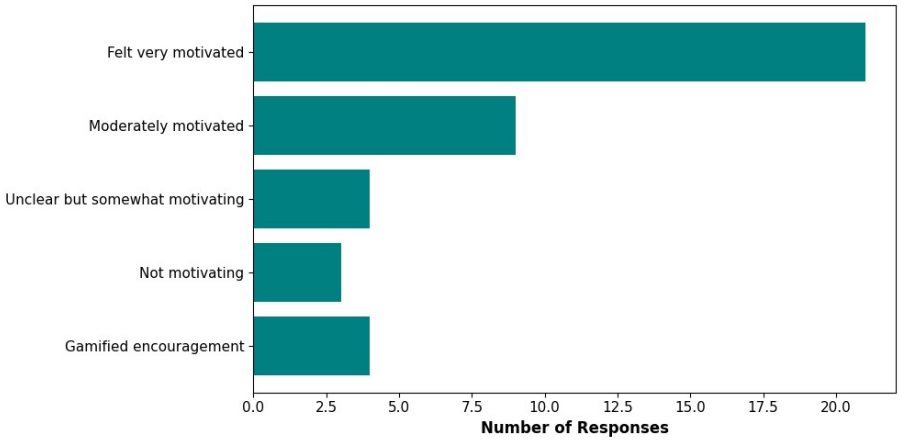


Figure 7.12: Motivation Gained Through Earning Points for Good Security Habits

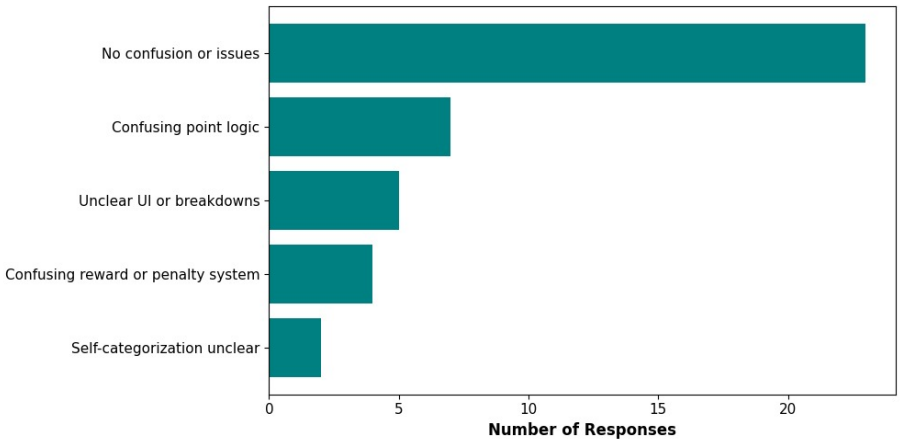


Figure 7.13: Confusing or Unnecessary Aspects Noticed in the Point System

not know what caused points to go down". Several individuals want increased transparency, particularly regarding the computation of scores. One proposed, "Maybe a clearer breakdown of point logic would help".

In conclusion, the point and reward system proved to be more than only a supplementary feature. It evolved into a behavioral catalyst, an element that facilitated user engagement, awareness, and motivation to maintain the security of their digital habits. While some users desired greater openness about point calculation, the function received commendation for its educational, enjoyable, and really beneficial nature. It instilled a sense of significance in users' actions, which is a substantial achievement for any privacy application.

Customization and Settings

The customization and settings tools were largely praised, with numerous users appreciating the power they provided over permission management. The majority of participants deemed the customization of permission categories to be both straightforward and pleasant. Users remarked on their ability to arrange applications based on personal criteria—"It's a good feature, like I can customize the categories according to my own preferences", stated one. Many characterized the process as

"relatively simple," "enjoyable," and "highly intuitive," however some noted the necessity of consulting the tutorial initially or experiencing initial confusion. A user remarked, "I did it after watching the tutorial". One user remarked, "It was easy actually" while another stated, "It was understandable after some time of using the app". Approximately 30 individuals deemed this method accessible, whereas just a minor subset reported challenges or avoidance.

Categorizing applications was often regarded as a time-efficient and organizational instrument. More than 30 participants indicated that the procedure facilitated the optimization of their applications, particularly in distinguishing between personal and professional usage. One stated, "Yes, assigning apps to categories helped organize everything better" while another commented, "Yes, grouping apps by category was helpful". A few, however, proposed that auto-categorization would improve convenience: "The process was a bit hectic and time-consuming", one remarked. These replies indicate that the function is effective yet might be enhanced with more intelligent defaults.

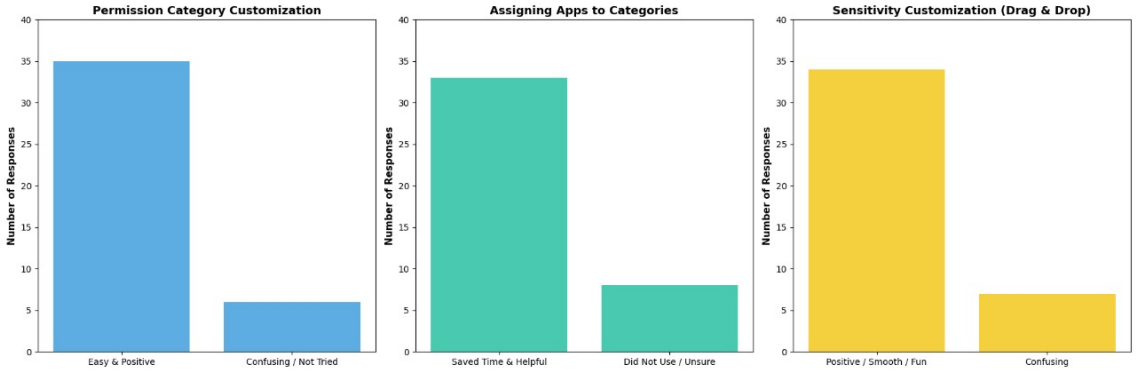


Figure 7.14: Users' Feedback on Permission Category Customization, Assigning Apps and Sensitivity Customizations

The Sensitivity Customization, especially the drag-and-drop interface, received commendation for its smoothness, interactivity, and intuitiveness. The tool was characterized as "fun", "great" and "very responsive" effectively fostering user engagement. One participant remarked, "It functioned seamlessly and enhanced the engagement of customization," while another described it as "a unique and useful option". Although some users saw performance delays or little uncertainty, the predominant sentiment—expressed by more than 30 users—was that the addition significantly enhanced the overall experience(Figure 7.14).

Users generally perceived the settings as beneficial and powerful, although suggested minor enhancements such as auto-sorting and further on-boarding guidance to minimize manual efforts. The amalgamation of flexibility, control, and engagement rendered this a distinguishing attribute for numerous individuals.

Learning and Usability

Analyzing initial user interactions with a privacy-centric application can provide significant insights on its accessibility and intuitiveness. During testing, the paper

investigated users' need for advice, identified their primary challenges, and assessed potential enhancements to the on-boarding process.

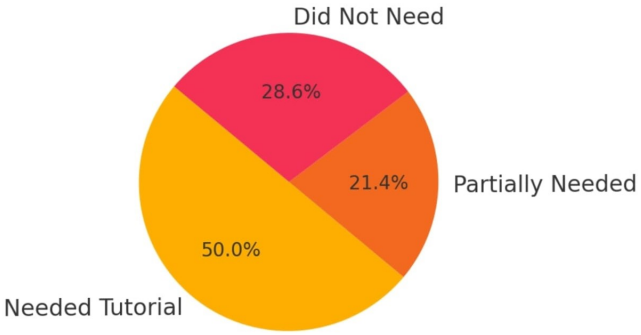


Figure 7.15: Whether Users Needed a Tutorial or Guidance to Understand the App

The responses about the necessity of a tutorial were polarized (Figure 7.15. Approximately fifty percent of the users indicated that they either viewed the training or required assistance at the outset. "Yes, I saw the tutorial video then I could use the app easily", one remarked. Others indicated that although they did not view a whole guide, they gained advantages from succinct explanations or assistance from colleagues. Simultaneously, around one-third indicated that the application was self-explanatory. "No, not at all. I figured it out quickly" remarked one user. This combination indicates that although the app is functional, alternative on-boarding could enhance initial engagement, particularly for users unfamiliar with app permissions or customization.

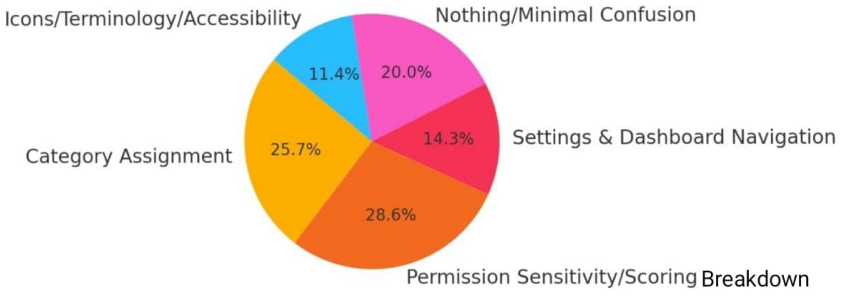


Figure 7.16: Features or Sections Users Found Most Difficult to Understand

In the investigation of identifying the most challenging aspects of the app, five primary sources of difficulty were revealed (Figure 7.16). The predominant issue was category assignment—users deemed it "tedious" or were unaware of its necessity. Numerous individuals indicated that the sensitivity settings and scoring system were initially ambiguous. Comments such as "Understanding the dashboard layout at first" and "all the scoring and permission customization was overwhelming" were commonplace. Several participants encountered difficulties with technical terminology, such as "sensitivity level" while others were unaware of aspects like permission customization until a later stage. The findings indicate that although the app design was largely effective, it is necessary to diminish ambiguity and enhance the visibility

of essential alternatives.

Nonetheless, the majority of users solicited enhanced in-app assistance, such as,

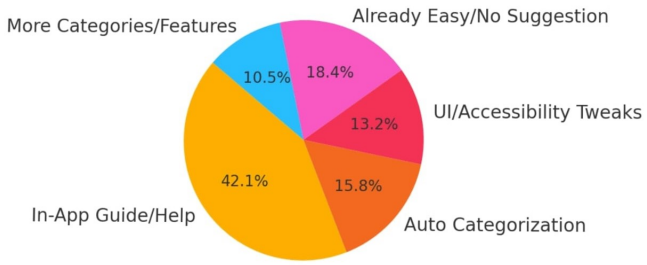


Figure 7.17: User Suggestions to Make the App Easier to Use

short tutorials, help buttons, or on-boarding slides (Figure 7.17). "An in-app guide or quick tip on first use would have helped", one stated. The second most prevalent recommendation was auto-categorization. While many valued manual control, they contended that automating the procedure may diminish setup time. Some requested enhanced accessibility features, such as enlarged text and a simplified layout, while others proposed the inclusion of score logic labels or explanatory notes. Significantly, several asserted that no enhancement was necessary. It is "Good to go already."

Behavior and Awareness

The primary aim of the app was to enhance privacy awareness and promote more responsible conduct around app permissions. According to participant evaluation, this objective was largely achieved.

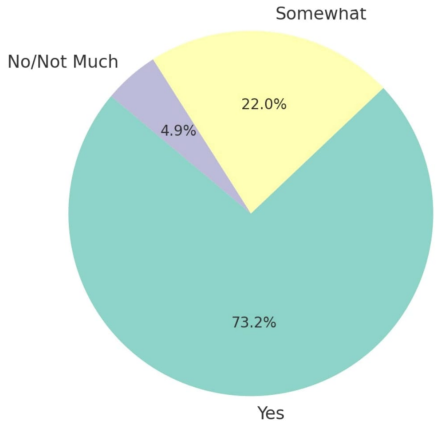


Figure 7.18: Change in User Attitude Towards App Permissions After Using the App

When asked about any alterations in their perspective on app permissions, the majority of participants affirmed a shift (Figure 7.18). This response unveiled the primary theme: Awareness Shift. Numerous individuals indicated that they now engage in more critical evaluation prior to permitting data access. One user stated, "Yes. this app made me aware" while another remarked, "I now double-check what apps ask for". A total of 30 participants reported a favorable adjustment in their mentality, whilst 9 indicated a partial change. Only two individuals reported that

the application had not produced a discernible impact. This indicates that even among users with increased privacy awareness, the application increased positive behaviors.

The second topic, closely associated with awareness, was the Sense of Control.

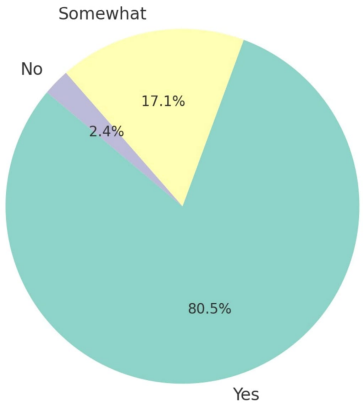


Figure 7.19: Users' Sense of Control Over Their Privacy After App Usage

From figure 7.19 the majority of participants (33 out of 41) reported feeling more empowered regarding their personal data following their use of the app. Many indicated that they had hitherto disregarded permission requests but were now attentive to them. One participant stated, "Yes, I know exactly what each app is doing" while another remarked, "I feel much more in control of my data now". This discovery confirms that the application effectively transitioned users from passive to active management of their digital privacy.

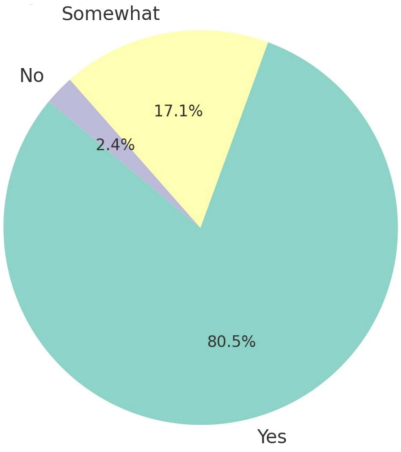


Figure 7.20: Increase in Carefulness About Trusted Apps After Using the App

The third key concept that emerged was Enhanced Vigilance Regarding Applications. The majority, 33 out of 41 respondents (Figure 7.20), affirmed that they are now more discerning regarding the apps they trust. One user stated, "I no longer install apps without checking permissions" while another remarked, "I uninstalled apps that seemed suspicious" These behaviors indicate that the app not only educated users but also prompted them to reevaluate existing applications and make more informed choices in the future. The pattern across these three inquiries is evident: the application enhanced users' alertness, knowledge, and intentionality.

Several users exhibited little alteration in their behavior; nevertheless, for the majority, the app functioned as a significant catalyst—prompting substantial action.

Overall Experience

User feedback on their entire experience with the mobile security application was predominantly favorable, exhibiting a continuous appreciation for several key aspects. Upon inquiry regarding their preferred aspect of the application, participants identified seven prevalent themes. They predominantly preferred the scoring and point-based system to enhance the interactivity of security. One participant stated, "Scoring was motivational," while another noted, "It gives scores on permissions, so people will be motivated to check permissions daily". This indicates that the point based scoring aspect was not just engaging but also significant in promoting secure behavior.

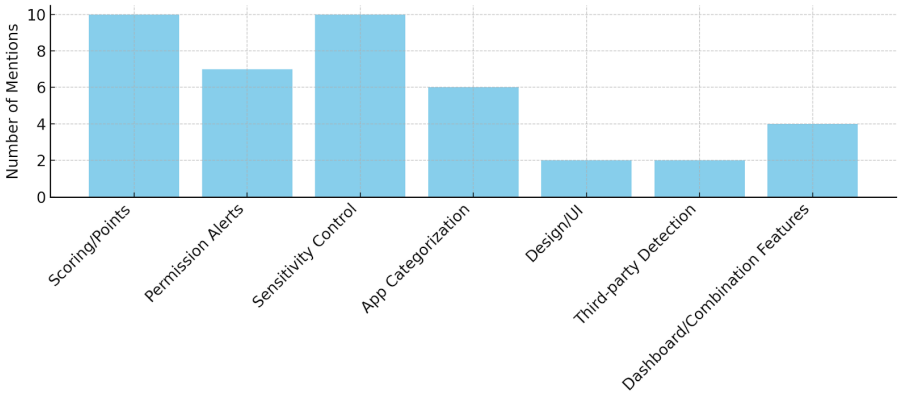


Figure 7.21: Users' Most Liked Features of the App and Reasons

The sensitivity control and customization features were highly commended (Figure 7.21). Numerous users described the drag-and-drop permission setting and nuanced sensitivity levels as powerful. A participant said, "The permission sensitivity customization gives much control on permission," while another expressed appreciation for the ability to "categorize independently". Others appreciated the comprehensive permission notifications, noting that they facilitated the identification of third-party applications or superfluous access. This transparency improved consumers' awareness of the underlying operations of their applications. A limited proportion valued the overall interface and design or deemed the integration of the dashboard and notifications especially successful.
From figure 7.22, in discussions regarding potential improvements, recommendations primarily focused on augmenting user-friendliness rather than rectifying fundamental functionality. The predominant request was for an in-app guide or lesson to assist new users in comprehending elements such as scoring and customization. Some indicated that automatic categorization applications might diminish manual labor, while others requested a more intuitive design or slight user interface enhancements. One user stated, "The numbering system needs clearer explanation" while another requested that the software be "more elder-friendly" Several individuals also noted the enhancement of sensitivity configuration and the incorporation of accessibility settings for increased use.

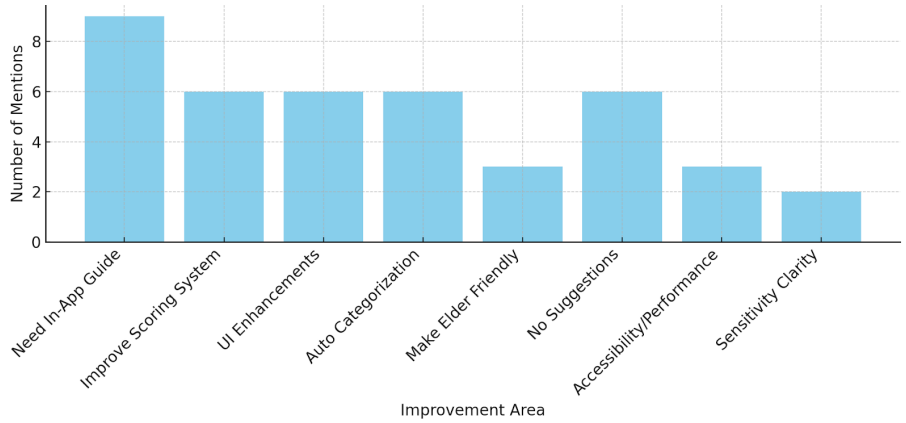


Figure 7.22: Users' Opinions on Which Parts of the App Need Improvement

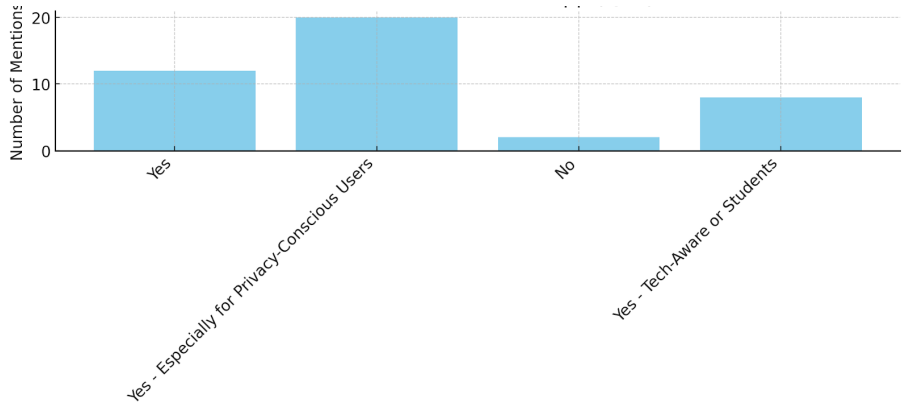


Figure 7.23: Whether Users Would Recommend the App to Others and Why

from figure 7.23, the feedback about the recommendation of the app to others was largely positive. The majority of participants affirmed positively, with several individuals indicating they had previously recommended it to friends, classmates, or family members. One user said, "Yes helpful, everyone should maintain phone safety" while others highlighted its utility for privacy-conscious users or those without technological proficiency. A few individuals expressed skepticism, believing the app was not essential for their personal use; nonetheless, they recognized its potential advantages for others.

In conclusion, the application achieved a harmonious equilibrium between functionality and ease of use. The preferred features, such as, scoring, notifications, customization etc corresponded effectively with users' aspirations for both control and information. The proposed enhancements emphasized refinement rather than redesign, signifying that the fundamental notion was positively acknowledged. The robust inclination to endorse the app significantly reflects its perceived value. These findings inform the future road-map and validate that the existing design addresses genuine user requirements.

Chapter 8

Discussion

Our thesis has been aiming to answer the research questions covered at the beginning of our paper. Some answers were retrieved from experiments found in the research papers of other researchers and have been addressed in our literature review. Others got their answers from the surveys and interviews we conducted from users who were given access to use and review our proposed solution. This chapter is designed to summarize the answers to all of the questions and to bring them all together in one place for convenience.

RQ1 – The Extent of Control an Average Smartphone User Has Over Personal Data

Our findings, grounded in both empirical survey results and research of existing literature, reveal that the average smartphone user possesses limited actual control over their personal data, despite the presence of technical privacy mechanisms within mobile operating systems. Although platforms like Android offer users a variety of tools for permission management, encryption, and application behavior oversight, these tools are seldom understood or utilized effectively by the general user population.

Survey responses demonstrated a widespread lack of awareness regarding mobile security features, with only 17% of respondents indicating they pay attention to app permissions during installation. More strikingly, a mere 3% could accurately answer comprehension questions related to permission usage. These figures point to a profound gap between the availability of control and users' capability or willingness to exercise it.

Our analysis of the current mobile ecosystem highlights several behavioral and structural limitations. Many users exhibit a high degree of implicit trust in applications, particularly those sourced from official app stores. This trust often results in the acceptance of excessive permission requests, thereby exposing users to unauthorized data access. This aligns with existing literature which reports that a large number of Android applications request more permissions than are functionally necessary, frequently accessing sensitive data such as contact lists, location history, and microphone input, often without the user's informed consent.

Despite the increasing availability of user-centric privacy controls, the complexity of permission interfaces and the prevalence of technical jargon hinder effective user engagement. Prior studies, supported by our own survey, affirm that most users either do not read or fail to understand permission prompts, especially those embedded within lengthy terms and conditions. Consequently, perceived control over personal data often masks a real and consequential lack of agency.

Further complicating the issue is the phenomenon of notification fatigue. Excessive or poorly contextualized notifications may lead users to disable these features altogether, thereby undermining their purpose. The success of privacy-enhancing tools thus depends not only on their technical accuracy but also on their usability and clarity.

Another dimension uncovered through our research pertains to shared device usage. Although smartphones are largely perceived as personal devices, our findings suggest that many users share them with others, either temporarily or regularly, introducing additional vectors for privacy loss. In such contexts, data access control mechanisms are underutilized, and privacy violations often go unnoticed.

Taken together, these insights indicate that while mobile platforms may offer the illusion of user control, actual control remains minimal without adequate user education and intuitive privacy mechanisms. By embedding privacy decisions into the user's everyday interactions and rewarding good security practices, we aim to transform passive awareness into active engagement, thereby enhancing the average user's ability to manage their personal data effectively.

RQ2 – Current User Perspectives and Carefulness Regarding App Permissions

Our research reveals a complex and often contradictory relationship between smartphone users and mobile application permissions. While users frequently express concern over data privacy, this concern does not consistently translate into careful or informed behaviors. The survey data, supported by extensive literature, indicates that the majority of users exhibit low engagement with permission management practices, suggesting a concerning gap between perceived importance and actual action.

In our survey, a significant portion of respondents reported that they rarely reviewed or managed app permissions during or after installation. Despite acknowledging the potential risks associated with excessive data access, many users admitted to granting permissions reflexively, often without reading the prompt in detail. This passive acceptance of permissions is partly influenced by overconfidence in app store curation—users presume that apps available on official platforms have already been vetted for security, thus minimizing the need for personal scrutiny.

Further, there is a prevailing assumption among users that permissions are only active while the app is in use. This misperception results in widespread underestimation of the privacy implications posed by background data collection. Even more

concerning is the finding that apps commonly perceived to be harmless, such as utility or entertainment applications, are often granted access to high-risk features like location, microphone, and contacts, often without legitimate justification. This aligns with prior studies noting that a substantial number of applications request permissions that extend beyond their functional scope.

From a behavioral standpoint, we observed reactive rather than proactive privacy practices. Users typically respond to permissions only after experiencing a privacy-related incident or upon receiving explicit alerts. This reactive posture may be attributed to interface complexity, terminology ambiguity, and the lack of contextual explanations provided during the permission granting process. As other scholars have noted, when permissions are presented using technical language or bundled with nonessential terms, users are more likely to bypass them entirely rather than assess their implications.

Our qualitative findings reinforce this behavioral pattern. Respondents frequently articulated a desire for more transparent, categorized permission warnings that would help distinguish essential access from suspicious or excessive requests. Additionally, they expressed support for a system that could provide real-time feedback on app behavior, suggesting that users are more likely to act cautiously when presented with dynamic and contextualized information rather than static and abstract permission prompts.

Very few users reported revisiting permission settings after installation, even when made aware of an app's unnecessary access patterns. This lack of follow-up suggests that many users view permission management as a one-time task rather than an ongoing responsibility.

Notably, the users' educational background and exposure to digital literacy were correlated with higher levels of permission scrutiny. However, even among more digitally literate respondents, there remained a tendency to trust brand reputation or app popularity over individual permission behavior; highlighting the role of social and psychological biases in user decision-making.

RQ3 – Existing Solutions and a Comprehensive Proposal to Address Privacy Theft, Unwanted Permission Access and User Engagement in Mobile Security

The challenges of protecting user data on smartphones are many-sided, encompassing unauthorized permission access and low user engagement with existing privacy tools. Through our literature review, system development, and user feedback, we identified a number of technical and behavioral solutions that have been proposed or implemented. However, our analysis also reveals a clear fragmentation in these approaches, as most existing solutions tend to target singular aspects of the problem rather than offering a unified strategy.
Furthermore, numerous studies have proposed categorized permission models, wherein permissions are grouped and analyzed contextually to determine their relevance to the app's stated functionality. This strategy supports automated detection of per-

mission misuse and provides an informative basis for alerting user. However, without an intuitive interface or ongoing user education, such systems may still overwhelm non-technical users.
To foster active user participation, incentive-based behavioral strategies have been explored. Point-based dashboards, badges, and quiz-based rewards have shown promise in fields like health and corporate cybersecurity. These interventions, while effective in encouraging short-term compliance, often suffer from engagement decay unless properly maintained and reinforced. Additionally, monetary incentives, though initially impactful, may fail to sustain behavior once removed, indicating the importance of non-financial, intrinsic motivators.
Despite these advancements, our findings suggest that the current ecosystem lacks an integrated approach that simultaneously addresses technical enforcement, user comprehension, and motivational engagement. To that end, our research proposes a unified mobile security system that leverages three core components:

1. Permission Monitoring and Categorized Alerts:

By providing immediate, context-sensitive notifications when applications require access to high-risk permissions (e.g., GPS, camera, microphone), our system bridges the gap between technical risk detection and user awareness. These alerts are tailored based on app category and usage context to avoid alert fatigue while maintaining transparency.

2. Point-Based Incentive and Security Dashboard:
Users are rewarded for completing secure actions such as managing permissions, updating apps, enabling two-factor authentication, and avoiding third-party app stores. This gamified framework promotes habitual engagement with security features and presents users with a visual metric of their "phone health," enhancing both motivation and comprehension.

3. **Privacy Risk Scoring:**
Our prototype analyzes app behavior against permission baselines, generating risk signals and prioritizing threats that merit user attention. This system not only identifies suspicious patterns in app behavior but also supports adaptive threat responses over time, integrating threat intelligence into a user-accessible interface.

Collectively, these features are designed to resolve the interconnected challenges of privacy theft, over-permissioned applications and low user involvement. By combining threat detection with behavioral incentives, our system transforms mobile security from a passive technical measure into an interactive, user-driven experience.

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.

RQ5 - Point-based 'phone health dashboard' system and its influence on user behavior in adopting secure practices, such as setting passwords and avoiding third-party apps

The integration of a point-based "phone health dashboard" system within the mo-

bile security application played a significant role in motivating users to adopt more secure digital practices. The resulting behavioral shifts, supported by both qualitative and quantitative findings, illustrate the transformative potential of incentivized security systems in mobile environments.

A dominant trend observed throughout user interactions was the effective influence on participation and retention. The point-based dashboard was repeatedly described by participants as "motivational" and "enjoyable," with multiple users drawing analogies between app usage and "playing a game." Such metaphors indicate that the system not only captured user interest but also sustained it over time, thereby enabling repetitive reinforcement of secure habits.

Quantitatively, the efficacy of the point system was evident in the security score improvements observed over a one-week period. The mean user score rose from 40 to 67.65, marking an average improvement of 27.65 points. Importantly, the highest individual score increase was 50 points, while only two users showed slight regressions. These metrics confirm that the dashboard served as a behavioral reinforcement, helping users transition from basic awareness to proactive engagement with their device's security settings.

Some users reported being unaware of their devices' vulnerabilities prior to engaging with the app. Upon receiving alerts tied to permissions and seeing how these impacted their scores, users became more vigilant. Specific instances were cited in which users revoked access to sensitive permissions (e.g., camera, GPS), deleted suspicious apps, and refrained from installing third-party applications altogether. One participant articulated this behavioral transformation by stating, "The app motivated me to remove suspicious permissions."

This shift was particularly evident in the interviews, where 11 users explicitly credited the point system for encouraging privacy-enhancing behavior, and an additional 13 reported a heightened awareness of their phone's security status. Participants were seen adopting behaviors like setting stronger passwords and managing permissions on a regular basis.

The point system also prompted users to re-evaluate their decision-making regarding third-party apps. Eight users specifically mentioned the third-party app detection feature, indicating that they had acted to revoke permissions or uninstall such apps in response to dashboard warnings.

While the point-based system was largely effective, the study also identified areas requiring refinement. Several users expressed confusion regarding the logic behind score allocation. The lack of clarity in how certain actions (e.g., disabling permissions) influenced the point total occasionally undermined trust in the system. As one user stated, "I was unaware of the factors that led to the decline in points." This highlights the necessity for increased transparency and guidance regarding the reward algorithm.

Moreover, some participants suggested that the dashboard could benefit from on-

boarding enhancements, such as in-app tutorials or tool-tips explaining the scoring mechanism. A clearer understanding of the link between behaviors and point changes could further reinforce the app's functionality of increasing awareness and enhance long-term engagement.

RQ6 - Usability challenges and user acceptance levels of a mobile security app that integrates live monitoring, permission warnings and a point-based reward system

The live monitoring, permission warnings, and a point-based reward system developed as the most important features of the app by the users. Many users were surprised to find how frequently applications, such as Bkash or Uber or Calculator, got unnecessary permissions. The live monitoring system, which provided users with concise, intelligible notifications concerning potentially sensitive or excessive permissions, assisted in bridging the awareness-to-action gap. It served as a protective and instructional tool, turning live monitoring from passive to active. According to 14 participants, notifications made them realize that programs like picture editors or calculators were asking for more access . "Helped me understand the unnecessary permissions on my phone and application-related security," one user said.

Live monitoring has proven indispensable in the contemporary digital scenery, as applications frequently access user data in the background without explicit agreement. The app provided transparency by monitoring permissions in real-time and promptly notifying users, enabling them to recover control and make educated decisions regarding the permissions they choose to grant or remove.

The point-based incentive system is a unique element designed to enhance the engagement of privacy management. Point-based positive privacy practices encouraged users to engage more often with the application and crucially, transformed sophisticated security principles into more measurable, enjoyable tasks. Many users reported that this approach increased their awareness of their digital behaviors. One user said, "The point-based reward system helped me understand how safe my phone is." Some said it made them "more aware of permission access" or "get rid of permissions that do not seem right." The results show that a large group (13 out of 39) said they knew more about their phone's security, and 11 said that this point-based reward system directly motivated them to take privacy-related actions. Many users liked how the experience felt like a game. One said, "Felt like game progress," which shows that security tasks became more fun. Although some participants sought further clarification on the calculation of points, the majority concurred that the feature effectively promoted secure behaviors.

Despite these advantages, there were also clear usability issues. The initial onboarding process was challenging for many users, particularly those who were less acquainted with permission customization or application categorization. Some users deemed the software intuitive, but others necessitated instruction, highlighting the requirement for more lessons or in-app support. The technical vocabulary associated with features such as sensitivity levels or category assignment hindered comprehensive understanding, especially during the initial stages of user experience.Seven

participants reported concerns over Technical Language or Vague Alerts, with one stating, "Some messages were excessively technical for me."

However, user adoption of integrated features such as live monitoring, permission alerts and point-based rewards were ultimately very high. Participants appreciated the system's transparency, sense of control and motivational aspects. They conveyed confidence in the application and felt encouraged by its clarity and use. Enhancing the on-boarding experience and clarifying difficult technical terminology could further improve accessibility and foster long-term engagement.

In an era characterized by discrete yet enduring mobile threats, the integration of live data monitoring ,real-time permission alerts and point-based incentives represents an effective trio. Collectively, they not only safeguard the device but also engage the user in the protection of their digital environment, transforming privacy from a mere expectation into an active practice.

RQ 7- Improvement or impact on user's lives after using our app

The results of our study demonstrate that after using our app, users' lives significantly and positively improved. The mobile security app influenced users' digital behavior, security awareness and overall sense of control. Prior to utilizing the application, many participants acknowledged that they had underestimated privacy features, frequently bypassing permission requests or naively placing trust in applications. Nonetheless, upon engagement with the system, a significant alteration occurred in users' perceptions and reactions to privacy-related decisions.

A notable enhancement was the transformation in awareness. After using the app, most users (33 out of 41) said they felt more in control of their personal information. Many said they were now paying attention to permission requests, which they had previously ignored. "Yes, I am now fully aware of the functionality of each application," said one participant. "I now feel significantly more in command of my data," said another. The application served not merely as a tool, but as a catalyst for a shift in thinking. A significant number of users indicated an increased awareness regarding the rights requested by applications and crucially, the potential unneeded or hazardous nature of those permissions. This shift in mindset manifested in proactive actions, including the examination of permissions prior to installation, routine verification of access configurations, and the removal of applications deemed dubious or obtrusive.

The sense of control consumers have over their personal information was a key area for improvement. People who had previously done little to protect their mobile privacy have started doing so actively. Users could understand the data being accessed as well as how to change or limit that access thanks to the application. In the modern digital world, where privacy issues can arise inside seemingly harmless applications, this sense of control is crucial.

In addition to fostering awareness and control, the app also promoted more prudent and deliberate decision-making. Users reported being more selective about which

apps to download and which apps to trust, with many reevaluating their current app collections and removing apps with disproportionate or unnecessary rights. “I no longer install applications without verifying permissions,” said one user, and “I uninstalled applications that looked suspicious,” added another. These actions show that in addition to educating users, the app encouraged them to reconsider already-existing apps and make better decisions going forward. This demonstrates a clear shift in behavior from reactive to preventative, users stopped only fixing problems and started actively avoiding them.

The point-based reward system enhanced behavioral change, which made admirable privacy habits rewarding and significant. We evaluated 41 users’ security scores before and after using the app for a week in order to assess changes in user behavior. Users initially demonstrated a basic awareness of mobile security with an average score of 40. The average score rose to 67.65 after a week of using features including the incentive system, sensitivity categorization and authorization notifications. The majority of users improved significantly; some even gained as much as 50 points. Due to decreased interaction, just two users experienced small reductions. The app’s ability to encourage safer mobile practices and ongoing privacy awareness is demonstrated by the average improvement of 27.65 points. Converting security practices into measurable improvements increased user motivation and engagement. The point-based reward system made an boring or technical task more enjoyable, which improved user retention and raised privacy settings engagement.

Users also appreciated elements that allowed them to customize their experience based on their own needs, like permission customization and sensitivity control. This adaptability made security a personal tool rather than just a collection of rules, empowering people rather than limiting them. This effect was enhanced by the simple design and educational notifications, which gave users knowledge about the events on their devices as well as their importance.

In the end, the application has the potential to significantly improve users’ digital life security. It gives clients the information they need to identify risks, the tools to lessen them, and the motivation to keep making improvements in their online safety. A significant number of users expressed that they are willing to recommend the application to others, underscoring its perceived worth and dependability.

This application not only improves user security but also cultivates a more resilient, privacy-conscious digital culture where users take responsibility for their own data in an environment where digital threats are sneaky, persistent and often ignored. By altering unnecessary access, raising awareness and offering simple operation, this app makes privacy protection both possible and empowering for everyday users.

Chapter 9

Conclusion

With smartphones taking an important place in both personal and professional life in the modern world, the security of mobile devices has become more and more complicated. Smartphones are not just communication tools, they contain sensitive personal data, financial transactions and browser access to all sorts of online activity, from emails to social media to cloud services. This creates a great risk as mobile devices become the tempting targets for cybercriminals. Growing number of smartphone apps that require permissions as well as an increasing volume of personal data stored on smartphones are creating huge privacy concerns.

The thesis highlights the issues surrounding mobile security, notably the lack of user engagement and awareness about what permissions the mobile applications ask for. Although technology advances in mobile security, such as encryption and biometric authentication, continue, users generally remain passive or unaware of the risk their mobile behaviors introduced. They give apps permission without fully understanding the security risks, making it easy for them to access user information without permission as well as spreading malware, phishing or causing identity theft. The problem is not as much in the technology as is the users' consciousness and how they interact with mobile security features.

This thesis clarifies the requesting of unnecessary permissions by mobile applications as a widespread problem. Since many users are willing to grant these permissions for convenience or simply lack of understanding, they do not think of the possible security risks. For example a flashlight app might ask for access to a user's contact list (clearly not needed by a flashlight app) or microphone (a permission that does not seem to be related to its functionality). This behavior may lead to malicious apps abusing these permissions and stealing personal info or tracking user activity.

This thesis clarifies the requesting of unnecessary permissions by mobile applications as a widespread problem. Since many users are willing to grant these permissions for convenience or simply lack of understanding, they do not think of the possible security risks. For example a flashlight app might ask for access to a user's contact list (clearly not needed by a flashlight app) or microphone (a permission that does not seem to be related to it's functionality). This behavior may lead to malicious apps abusing these permissions and stealing personal info or tracking user activity.

User privacy and security, being critical to the operation of this research, was highlighted as being dependent on permission based warning systems. One of the major data breaches in mobile app permissions is that users either ignore or misinterpret them. Categorization of permissions allows users to see which permissions are required for app functionality and which could pose a risk to their data. It has been shown that users tend to ignore warnings or do not care about what permissions they allow access to. These security systems give users the ability to decide for themselves what data they give out to applications, by giving them clear and concise information about what app permissions they are granting.

Additionally, the research explored the idea of using reward or incentive based systems to get users to interact with security protocols in a more engaging way. Behavioral economics teaches that positive reinforcement such as getting points or badges for securing personal data are more effective for motivating secure behavior than punitive measures. Implementation of these mechanisms ensures that this approach aligns security practices with user participation. Several studies supported the concept further by showing how rewarding users can drive their compliance with security measures, especially in organizational settings.

9.1 Research Limitation

Despite the useful insights obtained from this research, some limitations were recognized that may have affected the scope and usefulness of the findings. The survey and user testing were performed on a limited sample size within a certain demographic. The participants were predominantly highly tech-savvy university students, excluding a wider and more diversified demographic. Elderly adults and non-technical users were notably excluded from the study, hence constraining the generalisability of the findings across various demographics and levels of technology proficiency.

Secondly, some user remarks highlighted the lack of an in-app lesson or guidance system. Although many users were capable of using the app on their own, few indicated a requirement for detailed instructions to comprehend and effectively utilize the permission control functionalities. A further stated concern was the difficulty in understanding the security score in the security assessment feature. Certain users perceived the approach as perplexing or burdensome, prompting recommendations for a better scoring system and an UI design which is easy to understand for all demographics of users. Another mentioned difficulty was understanding the permission sensitivity categorization system. Some users found it perplexing or baffling how it works and demanded for an easy to use UI design or in-app guide for it.

Additionally, several users experienced inappropriate removal of essential permissions. This happened when the app denied permissions that were actually necessary for certain apps to run, which caused annoyance and decreased user pleasure. This is our drawback that users have to manually allow or deny permissions for some apps.

Another significant drawback is the prototype's dependence on the platform. The app was only built and tested on Android devices, rendering it unavailable to iOS or PC/laptop users. Consequently, potential platform-specific variances in permission

behavior could not be examined, and cross-platform compatibility remains an area for future study.

In conclusion, although the research significantly contributes to mobile permission awareness and control, its shortcomings must be rectified in future works to improve usability, inclusivity, and system efficacy.

9.2 Future Work

Based on the findings and constraints of this research, several possibilities for future exploration and advancement have been identified. The motive behind this research was to give an idea about permission management and real time tracking system, and it is recommended to implement this system in the operating system itself to use it with full potential. However as we cannot get the root access of the operating system we cannot implement or test all of the features. For example, to implement a real time permission tracking system we need the root access of the devices, but it is inconvenient as we cannot ask the users to root their phones in the user testing phase. If the system is integrated within the operating system it will work effectively. Also we were only able to implement it in android devices, there is a great opportunity for research for implementing in the IOS devices.

Another key area for enhancement is the broadening of the intended user demographic. Future research should encompass a more diverse demography, integrating participants from diverse age brackets, particularly senior citizens and persons with limited technological skills. This will facilitate the assessment of the system's usability and efficacy among a wider range of users and reveal usability problems that may not be evident within a technologically proficient student demographic.

Future iterations of the application should have an in-app interactive instruction or walkthrough to enhance the on-boarding experience. This feature will provide users with a step-by-step guide to the app's operation, hence improving comprehension and minimizing confusion, especially for novice or less experienced users.

Future endeavors should also prioritize the creation of an automatic permission categorization system, as indicated by user input. The system could utilize machine learning or rule-based logic to automatically assign permissions depending on application kind, usage patterns, or risk assessment, rather than demanding manual adjustments by users. This would enhance the system's user-friendliness and adaptability to specific requirements. Forthcoming implementations might also incorporate a more sophisticated UI design for the security assessment feature and permission sensitivity categorization.

Ultimately, future versions should prioritize real-time monitoring, a wider number of user base, cross-platform compatibility by extending the system to iOS, PC, web platforms etc and incorporate a user-friendly UI interface. That would markedly enhance its wide acceptance and influence, thereby making permission management a natural and essential component of daily mobile security protocols.

References

[1] N. Good, R. Dhamija, J. Grossklags, *et al.*, "Stopping spyware at the gate: A user study of privacy, notice and spyware," in *Proceedings of the 2005 Symposium on Usable Privacy and Security*, ser. SOUPS '05, Pittsburgh, Pennsylvania, USA: Association for Computing Machinery, 2005, pp. 43–52, ISBN: 1595931783. DOI: 10.1145/1073001.1073006. [Online]. Available: https://doi.org/10.1145/1073001.1073006.

[2] T. Herath and R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems*, vol. 47, pp. 154–165, May 2009. DOI: 10.1016/j.dss.2009.02.005.

[3] M. Mun, S. Hao, N. Mishra, *et al.*, "Personal data vaults: A locus of control for personal data streams," in *Proceedings of the 6th International COnference*, ser. Co-NEXT '10, Philadelphia, Pennsylvania: Association for Computing Machinery, 2010, ISBN: 9781450304481. DOI: 10.1145/1921168.1921191. [Online]. Available: https://doi.org/10.1145/1921168.1921191.

[4] J. Sun, Y. Fang, and X. Zhu, "Privacy and emergency response in e-healthcare leveraging wireless body sensor networks," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 66–73, 2010. DOI: 10.1109/MWC.2010.5416352.

[5] R. M. Villamarín-Salomón and J. C. Brustoloni, "Using reinforcement to strengthen users' secure behaviors," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '10, Atlanta, Georgia, USA: Association for Computing Machinery, 2010, pp. 363–372, ISBN: 9781605589299. DOI: 10.1145/1753326.1753382. [Online]. Available: https://doi.org/10.1145/1753326.1753382.

[6] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri, "Bridging the gap in computer security warnings: A mental model approach," *IEEE Security & Privacy*, vol. 9, no. 2, pp. 18–26, 2011. DOI: 10.1109/MSP.2010.198.

[7] A. P. Felt, K. Greenwood, and D. Wagner, "The effectiveness of application permissions," in *Proceedings of the 2nd USENIX Conference on Web Application Development*, ser. WebApps'11, Portland, OR: USENIX Association, 2011, p. 7.

[8] P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall, "These aren't the droids you're looking for: Retrofitting android to protect data from imperious applications," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, ser. CCS '11, Chicago, Illinois, USA: Association for Computing Machinery, 2011, pp. 639–652, ISBN: 9781450309486. DOI: 10.1145/2046707.2046780. [Online]. Available: https://doi.org/10.1145/2046707.2046780.

[9] P. H. Chia, Y. Yamamoto, and N. Asokan, "Is this app safe? a large scale study on application permissions and risk signals," in *Proceedings of the 21st International Conference on World Wide Web*, ser. WWW '12, Lyon, France: Association for Computing Machinery, 2012, pp. 311–320, ISBN: 9781450312295. DOI: 10.1145/2187836.2187879. [Online]. Available: https://doi.org/10.1145/2187836.2187879.

[10] A. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," *SOUPS 2012 - Proceedings of the 8th Symposium on Usable Privacy and Security*, Jul. 2012. DOI: 10.1145/2335356.2335360.

[11] A. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," *SOUPS 2012 - Proceedings of the 8th Symposium on Usable Privacy and Security*, Jul. 2012. DOI: 10.1145/2335356.2335360.

[12] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ser. SOUPS '12, Washington, D.C.: Association for Computing Machinery, 2012, ISBN: 9781450315326. DOI: 10.1145/2335356.2335360. [Online]. Available: https://doi.org/10.1145/2335356.2335360.

[13] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, "A conundrum of permissions: Installing applications on an android smartphone," in *Financial Cryptography and Data Security*, J. Blyth, S. Dietrich, and L. J. Camp, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 68–79, ISBN: 978-3-642-34638-5.

[14] M. Lane, "Does the android permission system provide adequate information privacy protection for end-users of mobile apps?," Jan. 2012.

[15] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang, "Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing," in *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, ser. UbiComp '12, Pittsburgh, Pennsylvania: Association for Computing Machinery, 2012, pp. 501–510, ISBN: 9781450312240. DOI: 10.1145/2370216.2370290. [Online]. Available: https://doi.org/10.1145/2370216.2370290.

[16] B. Sarma, N. Li, C. Gates, R. Potharaju, C. Nita-Rotaru, and I. Molloy, "Android permissions: A perspective combining risks and benefits," *Proceedings of ACM Symposium on Access Control Models and Technologies, SACMAT*, Jun. 2012. DOI: 10.1145/2295136.2295141.

[17] B. P. Sarma, N. Li, C. Gates, R. Potharaju, C. Nita-Rotaru, and I. Molloy, "Android permissions: A perspective combining risks and benefits," in *Proceedings of the 17th ACM Symposium on Access Control Models and Technologies*, ser. SACMAT '12, Newark, New Jersey, USA: Association for Computing Machinery, 2012, pp. 13–22, ISBN: 9781450312950. DOI: 10.1145/2295136.2295141. [Online]. Available: https://doi.org/10.1145/2295136.2295141.

[18] E. Struse, J. Seifert, S. Uellenbeck, E. Rukzio, and C. Wolf, "Permissionwatcher: Creating user awareness of application permissions in mobile systems," vol. 7683, Nov. 2012, pp. 65–80, ISBN: 9783642348976. DOI: 10.1007/978-3-642-34898-3_5.

[19] A. Anderson, D. Huttenlocher, J. Kleinberg, and J. Leskovec, "Steering user behavior with badges," in *Proceedings of the 22nd International Conference on World Wide Web*, ser. WWW '13, Rio de Janeiro, Brazil: Association for Computing Machinery, 2013, pp. 95–106, ISBN: 9781450320351. DOI: 10.1145/2488388.2488398. [Online]. Available: https://doi.org/10.1145/2488388.2488398.

[20] D. Van Bruggen, S. Liu, M. Kajzer, A. Striegel, C. R. Crowell, and J. D'Arcy, "Modifying smartphone user locking behavior," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ser. SOUPS '13, Newcastle, United Kingdom: Association for Computing Machinery, 2013, ISBN: 9781450323192. DOI: 10.1145/2501604.2501614. [Online]. Available: https://doi.org/10.1145/2501604.2501614.

[21] Y. Wang, J. Zheng, C. Sun, and S. Mukkamala, "Quantitative security risk assessment of android permissions and applications," in *Data and Applications Security and Privacy XXVII*, L. Wang and B. Shafiq, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 226–241, ISBN: 978-3-642-39256-6.

[22] T. August, R. August, and H. Shin, "Designing user incentives for cybersecurity," *Communications of the ACM*, vol. 57, pp. 43–46, Oct. 2014. DOI: 10.1145/2629487.

[23] W. Enck, P. Gilbert, S. Han, *et al.*, "Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones," *ACM Trans. Comput. Syst.*, vol. 32, no. 2, Jun. 2014, ISSN: 0734-2071. DOI: 10.1145/2619091. [Online]. Available: https://doi.org/10.1145/2619091.

[24] I. Liccardi, J. Pato, D. Weitzner, H. Abelson, and D. D. Roure, "No technical understanding required: Helping users make informed choices about access to their personal data," ICST, Nov. 2014. DOI: 10.4108/icst.mobiquitous.2014.258066.

[25] J. Lin, B. Liu, N. Sadeh, and J. I. Hong, "Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings," in *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, ser. SOUPS '14, Menlo Park, CA: USENIX Association, 2014, pp. 199–212, ISBN: 9781931971133.

[26] B. Liu, J. Lin, and N. Sadeh, "Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help?" In *Proceedings of the 23rd International Conference on World Wide Web*, ser. WWW '14, Seoul, Korea: Association for Computing Machinery, 2014, pp. 201–212, ISBN: 9781450327442. DOI: 10.1145/2566486.2568035. [Online]. Available: https://doi.org/10.1145/2566486.2568035.

[27] P. D. Meshram and R. Thool, "A survey paper on vulnerabilities in android os and security of android devices," in *2014 IEEE Global Conference on Wireless Computing Networking (GCWCN)*, 2014, pp. 174–178. DOI: 10.1109/GCWCN.2014.7030873.

[28] I. J. Mojica, B. Adams, M. Nagappan, S. Dienst, T. Berger, and A. E. Hassan, "A large-scale empirical study on software reuse in mobile apps," *IEEE Software*, vol. 31, no. 2, pp. 78–86, 2014. DOI: 10.1109/MS.2013.142.

[29] M. Vescovi, C. Perentis, C. Leonardi, B. Lepri, and C. Moiso, "My data store: Toward user awareness and control on personal data," *UbiComp 2014 - Adjunct Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pp. 179–182, Sep. 2014. DOI: 10.1145/2638728.2638745.

[30] W. Wang, X. Wang, D. Feng, J. Liu, Z. Han, and X. Zhang, "Exploring permission-induced risk in android applications for malicious application detection," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 11, pp. 1869–1882, 2014. DOI: 10.1109/TIFS.2014.2353996.

[31] H. Almuhimedi, F. Schaub, N. Sadeh, *et al.*, "Your location has been shared 5,398 times! a field study on mobile app privacy nudging," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '15, Seoul, Republic of Korea: Association for Computing Machinery, 2015, pp. 787–796, ISBN: 9781450331456. DOI: 10.1145/2702123.2702210. [Online]. Available: https://doi.org/10.1145/2702123.2702210.

[32] H. Almuhimedi, F. Schaub, N. Sadeh, *et al.*, "Your location has been shared 5,398 times! a field study on mobile app privacy nudging," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '15, Seoul, Republic of Korea: Association for Computing Machinery, 2015, pp. 787–796, ISBN: 9781450331456. DOI: 10.1145/2702123.2702210. [Online]. Available: https://doi.org/10.1145/2702123.2702210.

[33] M. Busch, S. Patil, G. Regal, C. Hochleitner, P. Fröhlich, and M. Tscheligi, "Persuasive information security: A behavior change support system to help employees protect organizational information security," Jun. 2015.

[34] J. Kang, D. Kim, H. Kim, and J. H. Huh, "Analyzing unnecessary permissions requested by android apps based on users' opinions," in *Information Security Applications*, K.-H. Rhee and J. H. Yi, Eds., Cham: Springer International Publishing, 2015, pp. 68–79, ISBN: 978-3-319-15087-1.

[35] S. K. Singh, B. Mishra, and P. Gera, "A privacy enhanced security framework for android users," in *2015 5th International Conference on IT Convergence and Security (ICITCS)*, 2015, pp. 1–6. DOI: 10.1109/ICITCS.2015.7292926.

[36] M. Tsavli, P. Efraimidis, V. Katos, and L. Mitrou, "Reengineering the user: Privacy concerns about personal data on smartphones," *Information Computer Security*, vol. 23, pp. 394–405, Jan. 2015.

[37] E. Chan, R. Kwortnik, and B. Wansink, "Mchealthy: How marketing incentives influence healthy food choices," *Cornell Hospitality Quarterly*, vol. 58, Sep. 2016. DOI: 10.1177/1938965516668403.

[38] M. Fagan and M. M. H. Khan, "Why do they do what they do? a study of what motivates users to (not) follow computer security advice," in *Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security*, ser. SOUPS '16, Denver, CO, USA: USENIX Association, 2016, pp. 59–75, ISBN: 9781931971317.

[39] S. Bu-Pasha, A. Alén-Savikko, J. Mäkinen, R. Guinness, and P. Korpisaari, "Eu law perspectives on location data privacy in smartphones and informed consent for transparency," *European Data Protection Law Review*, vol. 2, no. 3, 2016. DOI: 10.21552/EDPL/2016/3/7. [Online]. Available: https://doi.org/10.21552/EDPL/2016/3/7.

[40] Y. Zhou, T. Xu, A. Raake, and Y. Cai, "Access control is not enough: How owner and guest set limits to protect privacy when sharing smartphone," in *HCI International 2016 – Posters' Extended Abstracts*, C. Stephanidis, Ed., Cham: Springer International Publishing, 2016, pp. 494–499, ISBN: 978-3-319-40548-3.

[41] M. Alenezi and I. Almomani, "Abusing android permissions: A security perspective," in *2017 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT)*, 2017, pp. 1–6. DOI: 10.1109/AEECT.2017.8257772.

[42] M. Alsaleh, N. Alomar, and A. Alarifi, "Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods," *PLOS ONE*, vol. 12, Mar. 2017. DOI: 10.1371/journal.pone.0173284.

[43] H. Chen and W. Li, "Mobile device user's privacy security assurance behavior: A technology threat avoidance perspective," *Information and Computer Security*, vol. 25, Jul. 2017. DOI: 10.1108/ICS-04-2016-0027.

[44] A. Gheaus and V. Wild, "Introduction: Special issue on the ethics of incentives in healthcare," *Journal of Medical Ethics*, vol. 43, pp. 138–139, Mar. 2017. DOI: 10.1136/medethics-2016-104127.

[45] B. Krupp, D. Jesenseky, and A. Szampias, "Speproxy: Enforcing fine grained security and privacy controls on unmodified mobile devices," in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, 2017, pp. 520–526. DOI: 10.1109/UEMCON.2017.8248985.

[46] D. Naga Malleswari, A. Dhavalya, V. Divya Sai, and K. Srikanth, "A detailed study on risk assessment of mobile app permissions," *International Journal of Engineering amp; Technology*, vol. 7, no. 1.1, pp. 297–300, Dec. 2017. DOI: 10.14419/ijet.v7i1.1.9706. [Online]. Available: https://www.sciencepubco.com/index.php/ijet/article/view/9706.

[47] J. Pennekamp, M. Henze, and K. Wehrle, "A survey on the evolution of privacy enforcement on smartphones and the road ahead," *Pervasive and Mobile Computing*, vol. 42, pp. 58–76, 2017, ISSN: 1574-1192. DOI: https://doi.org/10.1016/j.pmcj.2017.09.005. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574119216304503.

[48] S. Ramachandran, A. Dimitri, M. Galinium, *et al.*, "Understanding and granting android permissions: A user survey," in *2017 International Carnahan Conference on Security Technology (ICCST)*, 2017, pp. 1–6. DOI: 10.1109/CCST.2017.8167834.

[49] Y. Zhou, A. Raake, T. Xu, and X. Zhang, "Users' perceived control, trust and expectation on privacy settings of smartphone," in *Cyberspace Safety and Security*, S. Wen, W. Wu, and A. Castiglione, Eds., Cham: Springer International Publishing, 2017, pp. 427–441.

[50] Y. Lu, C. Ou, and S. Angelopoulos, "Exploring the effect of monetary incentives on user behavior in online sharing platforms," Jan. 2018. DOI: 10.24251/HICSS.2018.436.

[51] A. Peruma, J. Palmerino, and D. E. Krutz, "Investigating user perception and comprehension of android permission models," in *Proceedings of the 5th International Conference on Mobile Software Engineering and Systems*, ser. MOBILESoft '18, Gothenburg, Sweden: Association for Computing Machinery, 2018, pp. 56–66, ISBN: 9781450357128. DOI: 10.1145/3197231.3197246. [Online]. Available: https://doi.org/10.1145/3197231.3197246.

[52] M. Rashid Idris, "Permission based risk assessment for enhancing privacy of android users," M.S. thesis, KTH, School of Electrical Engineering and Computer Science (EECS), 2018, p. 75.

[53] G. L. Scoccia, S. Ruberto, I. Malavolta, M. Autili, and P. Inverardi, "An investigation into android run-time permissions from the end users' perspective," in *Proceedings of the 5th International Conference on Mobile Software Engineering and Systems*, ser. MOBILESoft '18, Gothenburg, Sweden: Association for Computing Machinery, 2018, pp. 45–55, ISBN: 9781450357128. DOI: 10.1145/3197231.3197236. [Online]. Available: https://doi.org/10.1145/3197231.3197236.

[54] H. Elahi and G. Wang, "A participatory privacy protection framework for smart-phone application default settings," in *Security in Computing and Communications*, S. M. Thampi, S. Madria, G. Wang, D. B. Rawat, and J. M. Alcaraz Calero, Eds., Singapore: Springer Singapore, 2019, pp. 168–182, ISBN: 978-981-13-5826-5.

[55] M. Jutail, M. AL-Akhras, and A. Albesher, "Associated risks in mobile applications permissions," *Journal of Information Security*, vol. 10, pp. 69–90, Jan. 2019. DOI: 10.4236/jis.2019.102004.

[56] O. Olukoya, L. Mackenzie, and I. Omoronyia, "Permission-based risk signals for app behaviour characterization in android apps," Jan. 2019, pp. 183–192. DOI: 10.5220/0007248701830192.

[57] J. Brower, M. LaBarge, L. White, and M. Mitchell, "Examining responsiveness to an incentive-based mobile health app: Longitudinal observational study," *Journal of Medical Internet Research*, vol. 22, e16797, Aug. 2020. DOI: 10.2196/16797.

[58] S. Goel, K. Williams, J. Huang, and M. Warkentin, "Understanding the role of incentives in security behavior," Jan. 2020. DOI: 10.24251/HICSS.2020.519.

[59] B. P. D. Putranto, R. Saptoto, O. C. Jakaria, and W. Andriyani, "A comparative study of java and kotlin for android mobile application development," in *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 2020, pp. 383–388. DOI: 10.1109/ISRITI51436.2020.9315483.

[60] M. U. Shah, U. Rehman, F. Iqbal, F. Wahid, M. Hussain, and A. Arsalan, "Access permissions for apple watch applications: A study on users' perceptions," in *2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)*, 2020, pp. 1–7. DOI: 10.1109/CCCI49893.2020.9256714.

[61] R. Wang, Z. Wang, B. Tang, L. Zhao, and L. Wang, "Smartpi: Understanding permission implications of android apps from user reviews," *IEEE Transactions on Mobile Computing*, vol. 19, no. 12, pp. 2933–2945, 2020. DOI: 10.1109/TMC.2019.2934441.

[62] P. Mallojula, J. Ahmad, F. Li, and B. Luo, "You are (not) who your peers are: Identification of potentially excessive permission requests in android apps," in *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2021, pp. 114–121. DOI: 10.1109/TrustCom53373.2021.00033.

[63] G. Tangari, M. Ikram, I. W. B. Sentana, K. Ijaz, D. Kaafar, and S. Berkovsky, "Analyzing security issues of android mobile health and medical applications," *Journal of the American Medical Informatics Association : JAMIA*, vol. 28, Aug. 2021. DOI: 10.1093/jamia/ocab131.

[64] B. N. Lakshmi, A. Maaz, M. I. Khan, M. Mustafa, and S. A. M. N. Aziz, "Incentives for privacy-concerned mobile sensing systems," *International journal of health sciences*, vol. 6, no. S5, pp. 5405–5413, Jun. 2022. DOI: 10.53730/ijhs.v6nS5.9825. [Online]. Available: https://sciencescholar.us/journal/index.php/ijhs/article/view/9825.

[65] B. Mishra, A. Agarwal, A. Goel, *et al.*, "Privacy protection framework for android," *IEEE Access*, vol. 10, pp. 7973–7988, 2022. DOI: 10.1109/ACCESS.2022.3142345.

[66] F. D. Nocera and G. Tempestini, "Getting rid of the usability/security trade-off: A behavioral approach," *J. Cybersecur. Priv.*, vol. 2, pp. 245–256, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:247905488.

[67] Y. Shulman and J. Meyer, "Degrees of perceived control over personal information: Effects of information relevance and levels of processing," *IEEE Access*, vol. 10, pp. 40 596–40 608, 2022. DOI: 10.1109/ACCESS.2022.3167025.

[68] X. Zhan, T. Liu, L. Fan, *et al.*, "Research on third-party libraries in android apps: A taxonomy and systematic literature review," *IEEE Transactions on Software Engineering*, vol. 48, no. 10, pp. 4181–4213, 2022. DOI: 10.1109/TSE.2021.3114381.

[69] N. Alshomrani, S. Furnell, and Y. He, "Assessing user understanding, perception and behaviour with privacy and permission settings," in Jul. 2023, pp. 557–575, ISBN: 978-3-031-35821-0. DOI: 10.1007/978-3-031-35822-7_36.

[70] A. R. Javed, S. Abbas, T. Gadekallu, and Z. Muhammad, "Smartphone security and privacy: A survey on apts, sensor-based attacks, side-channel attacks, google play attacks, and defenses," *Technologies*, vol. 11, Jun. 2023. DOI: 10.3390/technologies11030076.

[71] M. Tahaei, R. Abu-Salma, and A. Rashid, "Stuck in the permissions with you: Developer & end-user perspectives on app permissions & their privacy ramifications," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, ser. CHI '23, Hamburg, Germany: Association for Computing Machinery, 2023, ISBN: 9781450394215. DOI: 10.1145/3544548.3581060. [Online]. Available: https://doi.org/10.1145/3544548.3581060.

[72] S. Yilmaz and M. Davis, "Hidden permissions on android: A permission-based android mobile privacy risk model," *European Conference on Cyber Warfare and Security*, vol. 22, pp. 717–724, Jun. 2023. DOI: 10.34190/eccws.22.1.1453.

[73] S. Prange, P. Knierim, G. Knoll, F. Dietz, A. D. Luca, and F. Alt, ""i do (not) need that feature!" - understanding users' awareness and control of privacy permissions on android smartphones," in *SOUPS @ USENIX Security Symposium*, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:272401881.

Appendix

TRACKO App

Figure 9.1 displays the home page which is you will see when you open the app. It displays the a personalized dashboard for your phone, it shows the points and danger level analyzing all the apps from your phone.

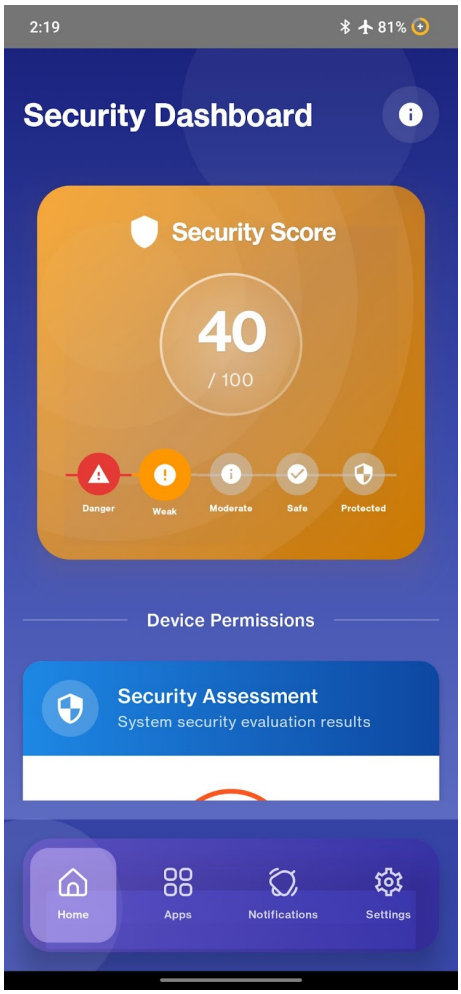


Figure 9.1: Security Dashboard

If you scroll down it will also show the condition of your device's password lock, biometric lock and third party apps like in figure 9.2.

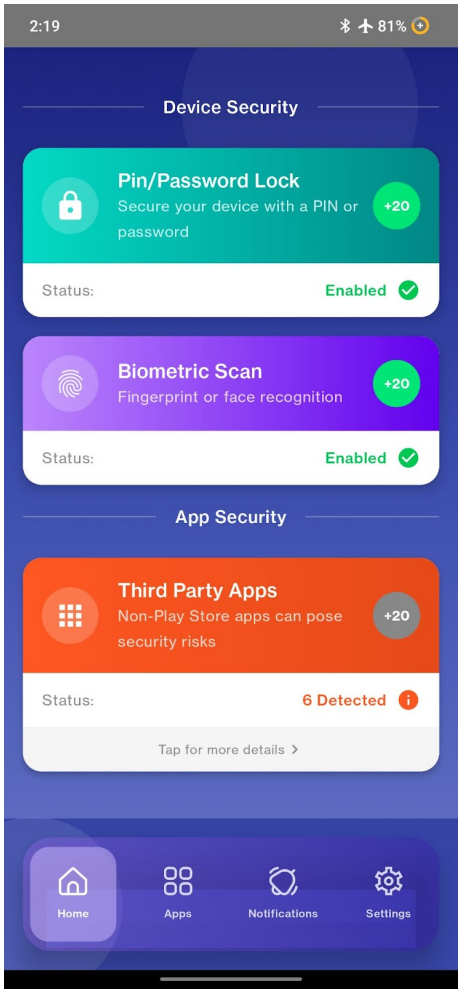


Figure 9.2: Detailed Security Dashboard

Figure 9.3 shows the 'Apps' section in the app, it basically shows what app is using what permission, it will also show a little warning in the left if the permission is risky or dangerous. You can change your permissions from here also you can select category for the app here.

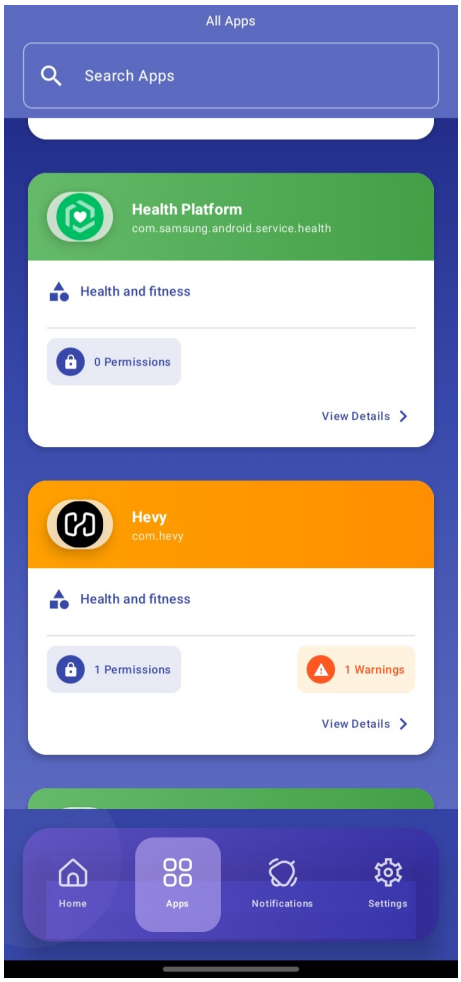


Figure 9.3: All the app's permission status

Figure 9.4 shows the notification section of the app. it shows all the unnecessary or risky permissions the apps in your device has taken. You can take necessary steps from here.

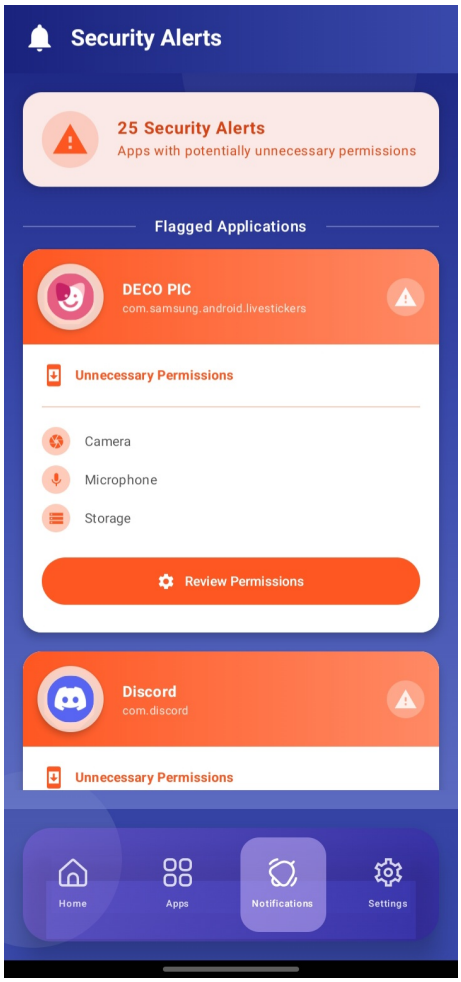


Figure 9.4: Notification

From the setting section, you can customize your app category according to your preference. In figure 9.5 you can assign apps to the existing categories or you can create a new one. Detailed visualization on how to add the categories and the permissions according to your preference is shown in figure 9.6 and figure 9.7

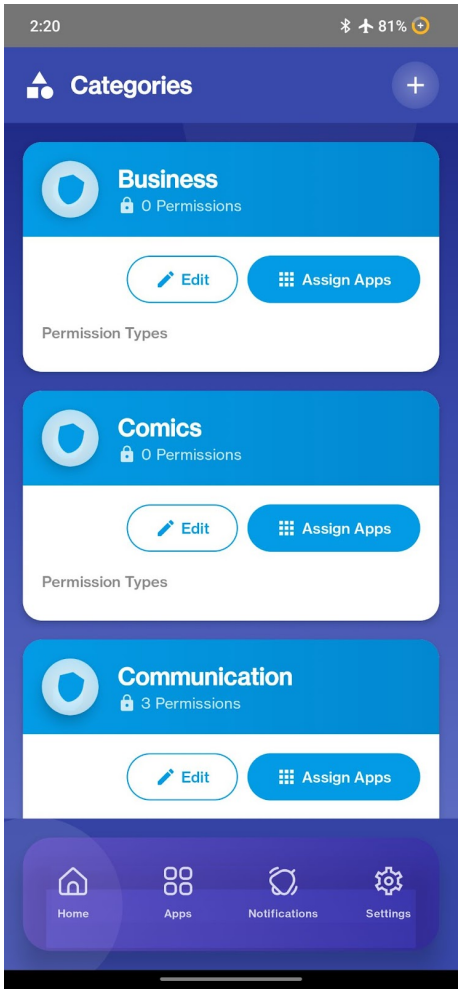


Figure 9.5: App Categorization

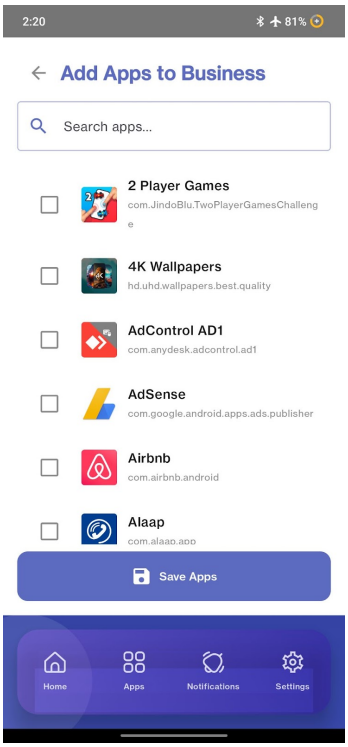


Figure 9.6: Adding apps to Category

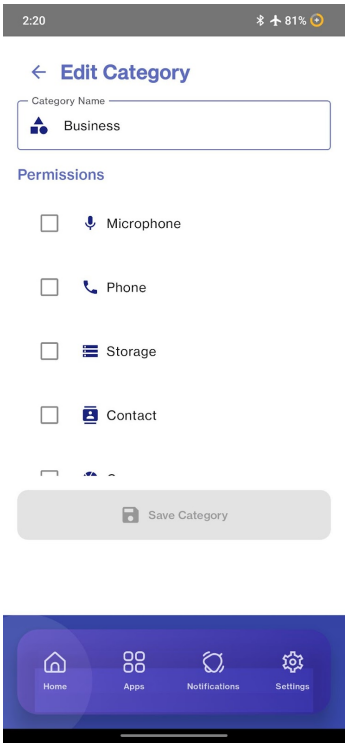


Figure 9.7: Editing Category

Figure 9.8 displays the sensitivity customization feature for 'TRACKO'. You can drag and drop the permissions according to your preference into 3 categories - High sensitivity, moderate sensitivity and low sensitivity. Your permission warnings and security points will adjust accordingly.

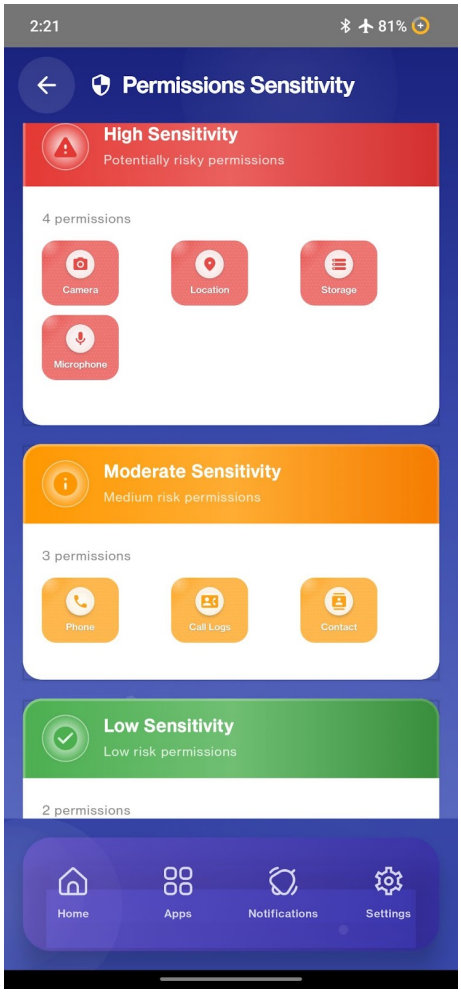


Figure 9.8: Sensitivity Customization

Pre Solution Survey Questionnaires

Welcome! We are conducting a brief 5-minute survey at BRAC University to enhance mobile security and user privacy. Your participation is voluntary and confidential. Help us understand your experiences with app permissions and contribute to impactful research. Thank you for your valuable insights!!!

Demographics

1. What is your age range?
    - Below 18
    - 18-24
    - 25-34
    - 35-44
    - 45+
2. What is your occupation?
    - Businessman
    - Corporate Worker
    - Household
    - Student
    - Unemployed
    - Labor
    - Self-employed
    - Teaching
    - IT Professional
    - Other: _____
3. How many hours a day do you spend on your smartphone?
    - Less than 2 hours
    - 2-4 hours
    - 5-8 hours
    - More than 8 hours
4. Which region do you belong to?
    - Rural
    - City

User Practices and Concerns About App Permissions

1. How often do you check app permissions before installing an app?
    - ○ Always
    - ○ Sometimes
    - ○ Rarely
    - ○ Never
2. Have you ever uninstalled or removed an app due to asking excessive permissions?
    - ○ Always
    - ○ Sometimes
3. How much trust do you place in apps on official app stores regarding permissions?
    - ○ High Trust
    - ○ Moderate Trust
    - ○ Low Trust
    - ○ Now Trust
4. How concerned are you about apps misusing permissions?
    - ○ Very Concerned
    - ○ Somewhat Concerned
    - ○ Not Concerned
5. What features would help you feel more secure about app permissions?
    - ☐ Instant alerts
    - ☐ Detailed permission breakdown
    - ☐ Educational resources
    - ☐ Other: _____
6. Where do you download most of your apps?
    - ○ Play Store
    - ○ App Store
    - ○ Other websites

Awareness and Engagement with Privacy Tools

1. Are you familiar with app permission control tools?
   - ○ Yes
   - ○ No
2. What would most encourage you to engage with app privacy?
   - ☐ Instant alerts
   - ☐ Reward based privacy system
   - ☐ In-app guides
   - ☐ Biometric access
   - ☐ Other: _____
3. Would you use an app that sends alerts about unnecessary or risky app permissions on your phone?
   - ○ Yes
   - ○ Maybe
   - ○ No
4. Have you ever searched for an app that warns you when other apps use your data, microphone, camera, or files unnecessarily?
   - ○ Yes
   - ○ No
5. What other measures would you suggest for protecting user data?

Post Solution User Study

Quantitative

1. Name: _____
2. Age:
    - Below 18
    - 18-24
    - 25-34
    - 35-44
    - 45+
3. Gender:
    - Male
    - Female
    - Other
4. Occupation: _____
5. Education Level:
    - Secondary school
    - Undergraduate student
    - Graduate
    - Employed
    - Other: _____
6. How long have you used a smartphone?
    - Less than 1 year
    - 1-3 years
    - 3-5 years
    - 5+ years
7. How many hours per day do you use mobile internet?
    - Less than 1 hour
    - 1-3 hours
    - 3-6 hours
    - 6+ hours
8. Before using this app, did you regularly check app permissions?
    - Always

- Sometimes
- Rarely
- Never

9. How concerned are you about mobile privacy?
    - Very Concerned
    - Somewhat Concerned
    - Not Concerned

System Usability Scale

1. I would like to use this app regularly.

	1	2	3	4	5	
Disagree	◯	◯	◯	◯	◯	Agree

2. I found the app easy to use.

	1	2	3	4	5	
Disagree	◯	◯	◯	◯	◯	Agree

3. I think I would need help to use this app.

	1	2	3	4	5	
Disagree	◯	◯	◯	◯	◯	Agree

4. The features were well arranged.

	1	2	3	4	5	
Disagree	◯	◯	◯	◯	◯	Agree

5. I had to learn many things before using it.

	1	2	3	4	5	
Disagree	◯	◯	◯	◯	◯	Agree

Ease Of Use

1. The permission alerts were easy to understand.

	1	2	3	4	5	
Not True	◯	◯	◯	◯	◯	True

2. The app helped me understand which permissions are necessary.

	1	2	3	4	5	
Not True	◯	◯	◯	◯	◯	True

3. The point system encouraged safe behavior.

	1	2	3	4	5	
Not True	◯	◯	◯	◯	◯	True

4. The dashboard helped me stay aware of my phone's security.

	1	2	3	4	5	
Not True	◯	◯	◯	◯	◯	True

5. The customization settings were easy to use.

	1	2	3	4	5	
Not True	◯	◯	◯	◯	◯	True

Qualitative

Permission Categorization

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

Point and Reward System

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

Customization and Settings

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

Learning and Usability

10. Did you need a tutorial to understand how the app works?
11. Which part was the hardest to understand?
12. How can we make this app easier to use for you?

Behavior and Awareness

13. Has your attitude toward app permissions changed after using this app?
14. Do you feel more in control of your privacy now?
15. Has this app made you more careful about which apps you trust?

Overall Experience

16. Which feature did you like most and why?
17. What part of the app needs improvement in your opinion?
18. Would you suggest this app to others? Why or why not?