Empirical Studies on Secure Development and Usage of Mobile Health Applications

Author: **Bakheet Aljedaani**

Principle Supervisor: Prof. Dr. Muhammad Ali Babar

Co-supervisor: Dr. Christoph Treude

A thesis submitted for the degree of Doctoral of Philosophy

in

Centre for Research on Engineering Software Technologies (CREST)
School of Computer Science
Faculty of Engineering, Computer and Mathematical Sciences
The University of Adelaide

February 2022

Contents

List of Figures

List of Tables

Abstract

Empirical Studies on Secure Development and Usage of Mobile Health Applications

By Bakheet Aljedaani

Mobile technologies, comprising portable devices, context-sensitive software applications, and wireless networking protocols, are being increasingly adopted to exploit services offered for pervasive computing platforms. The utilisation of mobile health (mHealth) apps in the healthcare domain has become a promising tool to improve and support delivering health services in a pervasive manner. mHealth apps enable health professionals and providers to monitor their patients remotely (e.g., managing patients with chronic diseases). mHealth apps enable expanding healthcare coverage (e.g., reaching places where little or no healthcare is available). Furthermore, mHealth apps were used to reduce the spread of disease and infection (e.g., the Covid-19 tracking apps). The use of mHealth apps will enhance the quality of healthcare, reduce the cost, and more convenient for patients. The security of mHealth apps becomes a significant concern due to the privacy and integrity of health-critical data. The interest of attackers in health-critical data (medical records, clinical reports, disease symptoms, etc.) has increased due to its value in the 'black market' as well as the social, legal, and financial consequences of compromised data.

This thesis focuses on understanding the security of mHealth apps based on (a) developers' and (b) end-users perspectives by conducting a set of empirical studies. To empirically investigate the existing research, a systematic literature review (SLR) was conducted to gain a deeper understanding of the security challenges, which hinder the development of secure mHealth apps. Based on the findings of the SLR, first, we conducted a survey-based study - involving 97 mHealth apps developers from 25 countries and six continents to investigate the practitioners' perspectives on security challenges, practices, and motivational factors that help developers to ensure the security of mHealth apps. Second, we conducted survey research - involving 101 end-users from two Saudi Arabian health providers to examine their security awareness about using clinical mHealth apps. We complement the end-users research by conducting an attack simulation study - involving 105 end-users from 14 countries and five continents to investigate their security behaviours when using mHealth apps.

The empirical studies in this thesis contribute to (i) providing developers' perspectives on critical challenges, best practices, and motivating factors that support the engineering and development of emerging and next-generation secure mHealth apps; (ii) providing empirical evidence and a set of guidelines to facilitate researchers, practitioners, and stakeholders to develop and adopt secure mHealth apps for clinical practices and public health; (iii) providing empirical evidence using action-driven measurement on human security behaviour when using mHealth apps, and presented the potential mechanisms that lead end-users to make improper security decisions.

Declaration

I, **Bakheet Aljedaani**, certify that this work contains no material which has been accepted for the award of any other degree or diploma in my name in any university or other tertiary institution and, to the best of my knowledge and belief, contains no material previously published or written by another person, except where due reference has been made in the text. In addition, I certify that no part of this work will, in the future, be used in a submission in my name for any other degree or diploma in any university or other tertiary institution without the prior approval of the University of Adelaide and where applicable, any partner institution responsible for the joint award of this degree.

I acknowledge that the copyright of published works contained within this thesis resides with the copyright holder(s) of those works.

I give permission for the digital version of my thesis to be made available on the web, via the University's digital research repository, the Library Search and also through web search engines, unless permission has been granted by the University to restrict access for a period of time.

Date: 22/02/2022

Acknowledgments

All praise is due to Allah as many times as the number of his creation, who allowed me to pass and achieve such a prestigious degree.

I would like to express my gratitude and appreciation to my principal supervisor, Professor Ali Babar, for the continuous support and guidance throughout my PhD candidature. I truly thank you, Professor Ali, for the insights, and useful discussions that motivated me to pick up the PhD and become who I am today.

I am grateful to Dr Aakash Ahmad for the extraordinary efforts he spent with me during the final stage of my PhD. His support and supervision helped me to improve the quality of research, and move forward in my PhD.

I would like to thank my co-supervisor Dr Christoph Treude, and Dr Mansooreh Zahedi for their significant support, especially during data collection and data analysis. It was an honour to have their feedback.

I would like to thank all my colleagues (CREST members). A special thanks to Dr Leonardo Iwaya, Dr Faheem Ullah, Dr Chadni Islam, Dr Nguyen Khoi Tran, Fangchao Tian, Triet Le, and Bushra Sabir for their helpful comments that improve the research papers during my PhD journey. I also would like to thank Dr Mahmoud Bokhari, and Dr Mojtaba Shahin for their support and care during my PhD.

I also want to express my sincere appreciation to Dr Emma Louise McEwin for her time to proofread the thesis.

I thank all the respondents who have volunteered their valuable time to involve in the studies and for sharing their experiences and views. It could not be possible without their contributions.

Special thanks to Umm Alqura University, Saudi Arabia, for offering me the PhD scholarship.

Last, but not least I would like to thank all my family members and friends for their support throughout the study. A special thanks to my beloved wife for being so supportive during the ups and downs of my PhD.

Dedication

To my extended family

Chapter 1

Introduction

Mobile computing is being leveraged to offer a multitude of context-aware services, ranging from social networking to fitness monitoring and smart healthcare [1]. Mobile devices unify (i) embedded sensors (for context-sensing), (ii) installed software (to process contextual data), and (iii) wireless networking (that transmits device data) to provide context-aware pervasive services. A recent report, 'The Mobile Economy 2020', published by GSMA [2] highlighted that by the end of 2019, 5.2 billion people (approx. 67% of the global population) subscribed to mobile services with an expected increase to 70% by 2025. Moreover, in 2019 mobile systems and services generated USD 4.1 trillion of economic value (approx. 4.7% of global GDP) with further growth expected to reach 4.9% by 2024. Mobile computing is revolutionizing the healthcare sector and becoming an integral part of smart healthcare initiatives offered to end-users via mobile health applications (known as mHealth apps) [3, 4]. mHealth apps forge connections between mobile technologies and the healthcare industry to provide a variety of low cost, efficient, and digitized healthcare services such as health and fitness monitoring [5], dermatologic care [6], chronic management [7, 8], and clinical practices [9]. Research2guidance (R2G), a leading consultancy firm for mHealth technologies, reported that 78,000 new mHealth apps were added to app stores in 2017 [10] with market revenue for digital health expected to reach USD 31 billion by 2020. An ever-increasing adoption of mHealth apps by healthcare stakeholders is evident in terms of 350,000 such apps available via application repositories of Android and iOS platforms [11].

The World Health Organisation (WHO) refers to mHealth as new horizons for health through mobile technologies [12] that facilitate stakeholders (e.g., governments, health units, medics, and patients) to provide or utilise health services in a pervasive, efficient, and automated manner. mHealth stakeholders rely on (a) mobile sensors to capture health-critical data, (b) mobile apps to process data, and (c) wireless networking to transmit data, regardless of geographical location or physical presence. For example, a patient with the help of a pre-installed mHealth app, without seeking a prior clinical appointment, could share his/her vital signs or lab reports for consultations with medical experts across the globe. From an operational perspective, mHealth tools, technologies such as wearable sensors, and apps support the outreach of healthcare professionals, neutralizing distance, time zones, and cost factors to provide accessible and affordable clinical practices.

1.1 Research Objectives and Questions

Despite the strategic benefits [13] and generated revenues [14], the security of health-critical data is among the topmost challenges for sustainability and mass-scale adoption of mHealth apps [1, 8, 15-18]. The risks of unauthorised access to health-critical data (e.g., disease symptoms, blood pressure, and clinical reports) are on the rise due to the value of data in the 'black market' along with the socio-legal consequences of the compromised data [19]. According to a recent report by the Ponemon Institute[1], the average price to maintain each medical record increased from USD 369 in 2016 to USD 380 in 2017 due to policies, regulations, and their implementations for securing health-critical data [20]. Medical records contain personal data (name, age, gender, address, contact detail etc.) and health-critical information (such as disease, prescriptions, treatment, etc.). This information could be used to embarrass the patients, could be used to have illegal drugs, receive treatment or make fake medical claims to insurance companies [21]. For mobile health systems, technical features alone may not be enough to ensure security, unless they are complemented with human-centric knowledge and practices to protect critical information. For example, a study by Mylonas et al. in 2013 [22] highlighted that mobile devices implement a multitude of security features including but not limited to device locks,

[1] Ponemon Institute available at https://www.ponemon.org/

remote data wipe, and end-to-end encryption. However, even the most sophisticated security features can never guarantee human behaviour (e.g., privacy leakage, unwanted access granted) that enhances or compromises device protection and/or data security [23, 24].

The app repositories provided by the world's leading and the most adopted app stores (i.e., Android and iOS with a joint market share of 99%) offer a multitude of mHealth apps and systems [10]. These apps vary, based on the type of mHealth services they offer and the granularity of health-critical data they collect, process, and exchange [11]. mHealth apps generally include, but are not limited to, health and fitness monitoring, medical consultations, clinical services, and medical imaging. As in Figure 1.1, despite the classification and healthcare services they offer, all of the mHealth apps rely on capturing personal data (age, gender, location etc.) and health-critical information (such as body temperatures, vital signs, and disease symptoms) that can be vulnerable to various security threats. Considering the context of mobile computing in general and mHealth systems in particular, security threats arise when attackers or malicious agents exploit existing vulnerabilities found in the operating system or in any third-party applications to gain access to the device resources and data [4]. Specifically, any tempering, selling to third parties, or breaching individuals' privacy of health-critical data can have serious social, legal, and financial consequences for both the app users and providers. Recently, some policies and regulations such as the European General Data Protection Regulation (EU GDPR) [25, 26] and the Health Insurance Portability and Accountability Act (HIPAA) [27, 28] enforce constraints on systems and ensure transparency of mechanisms that collect private data of end-users. Therefore, the security of mHealth apps become a significant issue due to the privacy and integrity requirements of health-critical data and the regulations to ensure that the privacy and integrity of personal data are maintained [5, 29].

Security vs. Privacy: Data security and privacy are often considered virtually synonymous terms, used interchangeably, referring to securing and/or protecting critical or classified information [30]. In mHealth systems, security and privacy of health-critical data are complementary concepts [30, 31]; however, for technical reasons, a distinction between the two must be maintained. Specifically, security refers to the implementation of practices and processes that ensure the confidentiality, availability, and integrity of health-critical data by restricting data usage or access by unauthorised entities [32]. In comparison, privacy has no absolute definition as it represents the basic human right (i.e., end-users' determination) about what, how much, when, and with whom to share information that is deemed as private to an individual (or a group) [33]. For example, in mHealth apps, privacy allows a user the right to grant or deny any access to their location, voice, contacts or health data; whereas security mechanisms such as anonymization, encryption, or data blockage enables privacy preservation. In this research, we focus on security of mHealth apps where privacy becomes implicit such as implementing security mechanisms to preserve/protect the privacy of the users.

Developers and end-users represent two actors with distinct but complementary roles to support the secure development and usage of mHealth apps, as illustrated in Figure 1.1. Developers focus on the

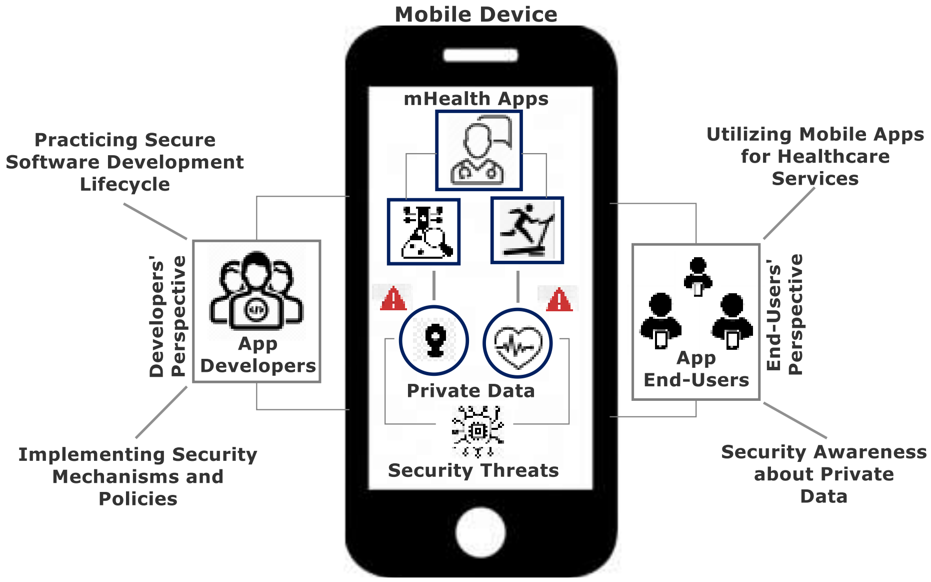

Mobile Device
mHealth Apps
Practicing Secure Software Development Lifecycle
Developers' Perspective
App Developers
Implementing Security Mechanisms and Policies
Private Data
Security Threats
Utilizing Mobile Apps for Healthcare Services
App End-Users
End-Users' Perspective
Security Awareness about Private Data

Figure 1.1 Overview of the Developers' and End-Users' Perspectives on Secure mHealth Apps

application of secure Software Development Lifecycle (SDLC) to engineer their apps that are secure and usable for end-users. Moreover, developers working in an individual capacity or as part of development teams are responsible for implementing the required security mechanisms (e.g., encryption, authentication, secure storage, and access control) and privacy policies to enhance the confidentiality and integrity of health-critical data [25-28]. A recent empirical study by Aljedaani et al. in 2020 [34] engaged a total of 97 mHealth app developers to investigate the challenges, motivating factors, and best practices to develop secure mHealth apps. The study provides a set of guidelines, and SDLC practices to develop security-aware apps, but highlights that even the most advanced security features may not be sufficient if end-users' lack security awareness about protecting their private information. As shown in Figure 1.1, end-users utilise the apps and developers most often assume that users' have appropriate security awareness (e.g., how to enable biometric authentication) regarding the use of mHealth apps. Security awareness enables end-users to understand the potential security threats (e.g., privacy leakage) and enable available countermeasures (i.e., rejecting excessive app permissions) to enhance the security and privacy of health-critical data. Lack of security awareness might lead to granting more permissions than necessary to unintentionally share health-critical data or allow other apps to unnecessarily access it [4].

Problem Statement: Whilst mHealth apps are considered a promising tool to improve the quality of healthcare services, security remains an issue that requires careful attention. mHealth apps' developers and end-users represent two actors to support secure development and usage of mHealth apps. On the one hand, failing to appropriately implement the basic security solutions (e.g., authentication, access control, and data encryption) by the developers has a huge impact on the security and privacy of health data. On the other hand, security awareness enables end-users to understand the potential security threats (e.g., privacy leakage) and enable available countermeasures (i.e., reject excessive app permissions) to enhance the security and privacy of health data. Lack of security awareness might lead to granting more permissions than necessary to unintentionally share health data or allow other apps to unnecessarily access it. Therefore, it is important to provide an evidence-based body of knowledge for practitioners and researchers to support research and development of emerging and next generation secure mHealth apps. Furthermore, it is important to investigate end-users' security awareness and behaviour towards using mHealth apps. Such an investigation helps to provide a set of guidelines to facilitate researchers, practitioners, and stakeholders to develop and adopt secure mHealth apps.

The overall objective of this thesis is to investigate the security of mHealth apps based on the developers' views (i.e., security challenges, security practices, and motivational factors); understand the security knowledge and perceptions of end-users when using mHealth apps (security knowledge, attitude, behaviour, security concerns, and security preferences); and understand the security behaviour of end-users when facing security threats (e.g., requesting permission to access device resources). This thesis is aimed to address the research questions presented in Table 1.1

Table 1.1 An Overview of Research Questions and Research Methods Used to Answer them

Study Focus	Research Question (RQ)	Chapter #	Associated Research Method
Developers' views of security of mHealth apps	**RQ1:** What are the reported challenges in literature that developers of mHealth apps face with respect to implementing security?	Chapter 3.1	Systematic Literature Review
	RQ2: What are the challenges that developers of mHealth apps face with respect to implementing security?	Chapter 4	Empirical Study
	RQ3: What motivates mHealth apps developers to develop secure mHealth apps?		
	RQ4: What security practices are used to incorporate security measures in mHealth apps?		
End-users' security knowledge and perception of mHealth apps	**RQ5:** What are the security knowledge and perceptions of end-users about using mHealth apps, which have been reported in the literature?	Chapter 3.2	Ad-hoc Literature Review
	RQ6: What is the level of security knowledge, attitude and behaviour of mHealth apps end-users about using mHealth apps?	Chapter 5	Empirical Study
	RQ7: What are the relationships between security knowledge, attitude and behaviour? And how do they influence the end-users of mHealth apps?		
	RQ8: To what extent are mHealth app end-users aware of the existing security features? And, what are the security features that mHealth app end-users wish to have in mHealth apps in the future?	Chapter 6	
	RQ9: What security issues have been faced by end-users during their usage of the employed security features within mHealth apps?		
	RQ10: What methods help end-users to improve their security knowledge regarding mHealth apps?		
End-users security behaviours towards using mHealth apps	**RQ11:** What are the security characteristics in the context of mHealth apps that we need to measure? And how they can be measured?	Chapter 3.3	Ad-hoc Literature Review
	RQ12: How do end-users react while facing potential security threats during the usage of mHealth apps?	Chapter 7	Empirical Study
	RQ13: What security-related mistakes do end-users make while using mHealth apps?		

1.2 Motivations

1.2.1 Developers' views of security of mHealth apps

Existing studies (e.g., [1, 8, 15-17, 35]) have found that the security of mHealth apps falls behind the capabilities of adversaries and the sophistication of cyber-attacks that target the apps. According to a recent study by Zhou et al. in 2019, despite the of benefits mHealth apps, their adoption is hampered by end-users' concerns about the security and privacy of their personal and health-critical information [23]. To address such issues, it is critical to conduct a research study about the challenges of developing secure mHealth apps, which are reported in the literature. In addition, it has become vital to investigate and understand the security of mHealth apps by incorporating practitioners' views on the challenges, best practices, and motivations to ensure secure mHealth apps. Such an investigation can help address some fundamental issues such as why mHealth apps are not secure, and what steps should be taken into consideration to improve the security.

1.2.2 End-users' security knowledge and perception of mHealth apps

The pervasive environment in which mobile devices continuously absorb health-critical data from embedded sensors, process data inside the device, and send it across ad-hoc networks makes mHealth app security a critical challenge [1, 36]. According to security experts, technical solutions such as authentication and multi-factor authorisation cannot address security issues alone; instead, the role of end-users and their understanding of security-related issues is essential to ensure secure mobile computing [37]. Some recent studies have highlighted that social engineering methods can be used by hackers to deceive end-users into leaking their private information [4, 38]. Thus, it is essential to investigate end-users' security knowledge, attitudes and behaviours regarding the use of mHealth apps. Furthermore, it is also essential to understand end-users' security awareness about the existing security features and how they become aware of such features, their security preferences that need to be employed, and the security issues they have experienced. The presented work in Chapter 4, and Chapter 5 complement the developers' views of the security of mHealth apps (Chapter 4) by empirically investigating end-users' security awareness about using mHealth apps that contain health-critical and other personal data.

1.2.3 End-users security behaviours towards using mHealth apps

As indicated in Section 1.2.2, the success factor of ensuring security in mHealth apps is significantly influenced by end-users' knowledge and actions [37]. End-users become a threat and can easily get deceived into releasing their health data if they are not fully aware of the security features which they are expected to use [4, 38]. This issue can be seen with technology-based solutions that involve using security features in such a way that end-users find them difficult to understand [39]. In regard to mHealth apps developers, they consider they have already delivered secure apps. However, end-users find these security features hard to understand and use [38]. The study presented in Chapter 5 [40] aimed to understand the security knowledge, attitude and behaviour of the end-users when using mHealth apps. The results revealed that end-users had the required knowledge of the security measures for the investigated apps, and that knowledge had a strong influence on their attitude. However, end-users' knowledge has not significantly influenced their behaviour, indicating that end-users are aware of risks but are reluctant or unaware of appropriate actions that mitigate risks. To further examine end-users' behaviours about the security of mHealth apps, an attack simulation approach study is conducted in Chapter 7 to understand their security awareness. The presented research in Chapter 7 extends and complements end-users' views about the security of mHealth apps (Chapter 5, and Chapter 6) by conducting an attack simulation approach study to measure the security awareness of end-users of mHealth apps. Such an investigation through action-driven measurement will help to understand end-users' reactions when they face security threats rather than focusing on self-reported behaviours.

1.3 Thesis Contributions

The key contributions of this thesis can be categorised into five areas:

1. A literature review about the security of mHealth apps (Chapter 3) which:
   - Identifies the challenges that hinder developers to develop secure mHealth apps.
   - Identifies end-users' security concerns towards using mHealth apps.

- Identifies the existing methods to measure the security awareness of end-users.

2. An empirical study with 97 mHealth apps developers about the security of mHealth apps (Chapter 4) which:
    - Identifies the challenges that prevent the development of secure mHealth apps.
    - Provides a taxonomy of the security practices for ensuring the security of mHealth apps.
    - Determines the motivational factors that encourage the developers of mHealth apps to develop secure mHealth apps.
3. Empirical evidence about the level of end-users' security awareness when using clinical mHealth apps through a survey of 101 end-users (Chapter 5) which:
    - Measures end-users’ security knowledge, attitude and behaviour towards using mHealth apps for clinical settings.
    - Illuminates the relationship between security knowledge, attitude, and behaviour and how they influence end-users while utilising mHealth apps.
4. Empirical exploration of end-users' security perceptions towards using clinical mHealth apps (Chapter 6) which:
    - Investigates end-users’ security awareness in terms of understanding of the existing features and desire for futuristic features that enable or enhance app security.
    - Provides a taxonomy and a benchmark to evaluate the effectiveness of security features offered by mHealth apps providers.
    - Reveals an empirically derived set of guidelines to facilitate researchers, practitioners, and stakeholders to develop secure and usable mHealth apps for clinical practices and public health.
5. A simulation-based attack with 105 end-users which measures end-users’ security behaviour (Chapter 7) to:
    - Understand the actual behaviour of end-users of mHealth apps instead of relying on the theoretical phenomenon (i.e., self-reported behaviour).
    - Identify the mistakes that lead to compromising end-users’ data during the use of mHealth apps.

1.4 Thesis outline and Publications

The core chapters of this thesis are derived from the publications which have been previously published or are currently under submission. It should be noted that I was responsible for all the studies conducted in this PhD thesis, most of them have been carried out through collaboration with my PhD supervisor and other collaborators. Hence, this PhD thesis uses “We” to refer to collaborative efforts. This PhD thesis explicitly distinguished the roles of the researchers whenever required. For example, when describing the qualitative data analysis, the present author is used to refer to the author of the thesis and other researchers are used to refer to others. Figure 1.2 shows an overview of the thesis scope and outline. The rest of this thesis is organised as follows:

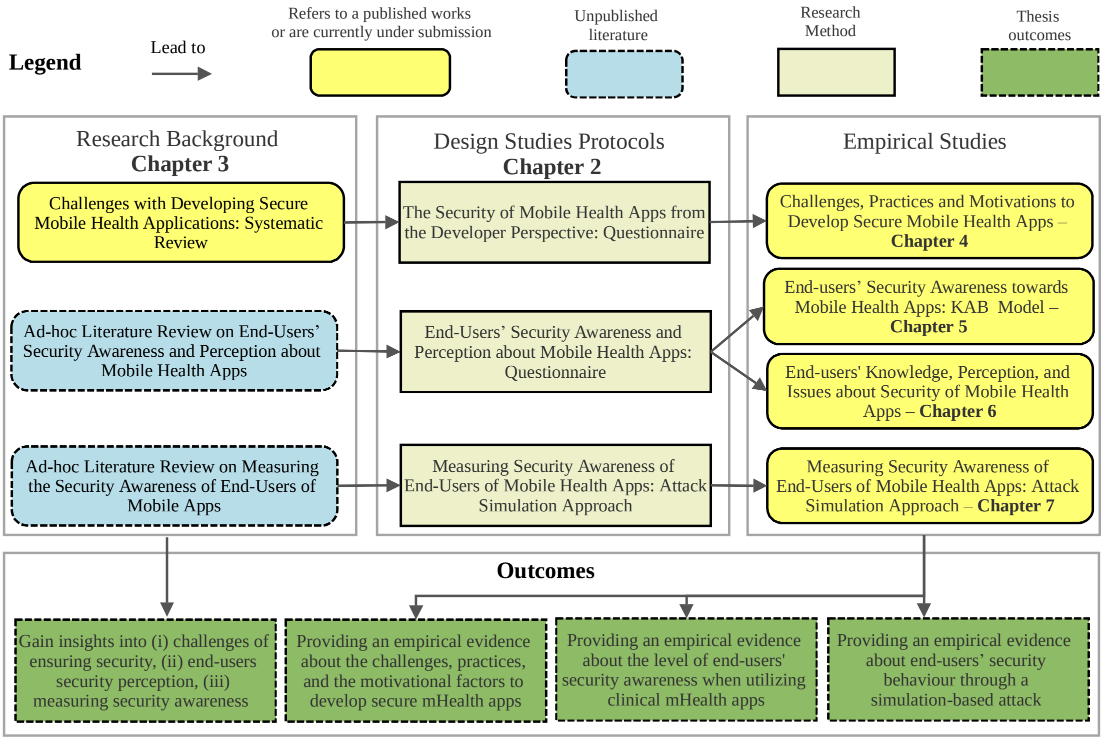

Legend
Lead to
Refers to a published works or are currently under submission
Unpublished literature
Research Method
Thesis outcomes
Research Background Chapter 3
Challenges with Developing Secure Mobile Health Applications: Systematic Review
Ad-hoc Literature Review on End-Users' Security Awareness and Perception about Mobile Health Apps
Ad-hoc Literature Review on Measuring the Security Awareness of End-Users of Mobile Apps
Design Studies Protocols Chapter 2
The Security of Mobile Health Apps from the Developer Perspective: Questionnaire
End-Users' Security Awareness and Perception about Mobile Health Apps: Questionnaire
Measuring Security Awareness of End-Users of Mobile Health Apps: Attack Simulation Approach
Empirical Studies
Challenges, Practices and Motivations to Develop Secure Mobile Health Apps – Chapter 4
End-users' Security Awareness towards Mobile Health Apps: KAB Model – Chapter 5
End-users' Knowledge, Perception, and Issues about Security of Mobile Health Apps – Chapter 6
Measuring Security Awareness of End-Users of Mobile Health Apps: Attack Simulation Approach – Chapter 7
Outcomes
Gain insights into (i) challenges of ensuring security, (ii) end-users security perception, (iii) measuring security awareness
Providing an empirical evidence about the challenges, practices, and the motivational factors to develop secure mHealth apps
Providing an empirical evidence about the level of end-users' security awareness when utilizing clinical mHealth apps
Providing an empirical evidence about end-users' security behaviour through a simulation-based attack

Figure 1.2 An Overview of the Thesis Scope and Organisation

Chapter 1: This chapter explains the motivations behind this thesis, the investigated research questions, the contributions of this research, and the organisation of this thesis.

Chapter 2: This chapter presents an overview of the adopted research methods to answer the outlined research questions in Table 1.1. It provides a detailed description of each research method including the reasons behind the chosen research method, the steps taken to design the research protocols, the methods of data collection, the performed techniques of data analysis and the limitations that could affect the research results.

Chapter 3: This chapter addresses the research questions ***RQ1***, ***RQ5***, and ***RQ11***. It presents the results of a systematic literature review to classify the challenges that hinder developers to develop secure mHealth apps (***RQ1***). Furthermore, it presents the results of a rigorous literature review to understand the security perceptions of end-users and their security concerns towards using mHealth apps (***RQ5***). Finally, it presents our findings on the methods which have been used in the literature to measure the security awareness of the end-users of mobile apps (***RQ11***). Section 3.1 in this chapter has been published as:

> ❶ **Bakheet Aljedaani**, M Ali Babar. 2021. *Challenges with Developing Secure Mobile Health Applications: Systematic Review*. JMIR mHealth uHealth 9, 6, e15654. DOI= http://dx.doi.org/10.2196/15654. [Impact Factor (2020): **4.31**, SJR rating: **Q1**]

Chapter 4: This chapter answers the research questions ***RQ2***, ***RQ3***, ***RQ4*** through a survey questionnaire study. First, it presents the challenges that the developers are facing to implement security. Second, it proposes a taxonomy for the security practices which have been followed by our participants. Third, it identifies mHealth apps developers' motivational factors for ensuring the security of mHealth apps. This chapter has been published as:

> ❷ **Bakheet Aljedaani**, Aakash Ahmad, Mansooreh Zahedi and Muhammad Ali Babar, *An Empirical Study on Developing Secure Mobile Health Apps: The Developers' Perspective*, 2020 27th Asia-Pacific Software Engineering Conference (APSEC), Singapore, Singapore, 2020, pp. 208-217, doi: 10.1109/APSEC51365.2020.00029. [Core rating: rank **B**, acceptance rate: **36%** (45/122)]

Chapter 5: This chapter provides answers to the research questions ***RQ6***, and ***RQ7*** through conducting a survey questionnaire study. First, it ascertains end-users' security knowledge, attitude, and behaviour towards utilising mHealth apps. Second, it investigates the correlation between their security knowledge, attitude, and behaviour and how these three dimensions affect each other. This chapter has been published as:

> ❸ **Bakheet Aljedaani**, Aakash Ahmad, Mansooreh Zahedi and Muhammad Ali Babar, *Security Awareness of End-Users of Mobile Health Applications: An Empirical Study*, presented at the MobiQuitous 2020 - 17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Darmstadt, Germany, 2020. [Core rating: rank **A**]

Chapter 6: This chapter answers the research questions ***RQ8***, ***RQ9***, and ***RQ10***, which were addressed through a survey questionnaire study. First, it presents end-users' preferred security features within mHealth apps. Second, it investigates the security issues that end-users experience. Third, it seeks to identify the methods which have been followed to increase the security awareness of end-users. This chapter has been submitted for publication:

> ❹ **Bakheet Aljedaani**, Aakash Ahmad, Mansooreh Zahedi and Muhammad Ali Babar, *End-Users' Knowledge and Perception about Security of Mobile Health Apps: A Case Study with Two Saudi Arabian mHealth Providers*, (under review): Journal of Systems and Software. [Impact factor (2020): **2.83**, Core rating: **A**]

Chapter 7: This chapter measures the security awareness of end-users' of mHealth apps to answer ***RQ12***, and ***RQ13***. This research was conducted through a simulation-based attack study. First, we prototyped a simulation app for the research purpose and developed one of the mHealth apps types. Second, we invited end-users to participate in our study to investigate what actions they perform to ensure the security of their health data, as well as investigate the mistakes they do. This chapter is going to be submitted for publication:

> ❺ **Bakheet Aljedaani**, Aakash Ahmad, Mansooreh Zahedi and Muhammad Ali Babar, *Investigating the Security Awareness of End-Users towards Using Mobile Health Apps: An Attack Simulation Approach* (to be submitted)

Chapter 8: This chapter concludes the thesis. It summarizes the key findings and proposes a few suggestions for future work.

Chapter 2

Research Method

This chapter presents the research methods pursued in this thesis. It starts with a brief explanation of the literature review and its goal, followed by a description of the survey questionnaire research method adopted for Chapters 4, 5, and 6. Finally, we describe the design of the simulation-based attack approach, which is used in Chapter 7.

2.1 Literature Review

As discussed in Chapter 1, we performed literature reviews to understand the existing research studies and to highlight the potential areas for investigation. We performed a Systematic Literature Review (SLR) to understand the developers' challenges in implementing secure mHealth apps. It is one of the most widely used research methods of Evidence-Based Software Engineering (EBSE) [41]. SLR provides a well-defined process for identifying, evaluating, and interpreting all available evidence relevant to particular research. An SLR involves three main phases: defining a review protocol, conducting the review, and reporting the review [42]. Furthermore, we performed an ad-hoc literature review to understand end-users' security concerns when using mHealth apps, and the existing mechanisms to measure end-users' security awareness towards using mHealth apps. Further details will be discussed in Chapter 3.

2.2 Developers’ Survey Questionnaire

In this section, we discuss the research method adopted for Chapter 4 which is comprised of four phases. Each phase is detailed below as per the illustrations in Figure 2.1. Furthermore, we point out some potential threats that might impact this study.

2.2.1 Phase I – Study Protocol and Questionnaire

We designed an online survey based on the findings of our systematic review (i.e., presented in Section 3.1, [43]), reviewing the literature (i.e., Section 4.2), and the guidelines of Kitchenham and Pfleeger [44]. As in Figure 2.1, we utilised an online platform (Google Forms) that is easy to share, view, and manage across platforms. In the survey preamble, we briefly described the purpose and eligibility of our study. The survey contained 14 Questions (**Q1** to **Q14,** available in Appendix B) designed to answer ***RQ2***, ***RQ3***, and ***RQ4*** (in Section 1.1). The link to the online survey is provided in [45]. **Q1**-**Q3** were screening questions to ensure that we engaged developers with experience with mHealth apps. Selecting the option of zero apps redirected the respondent to the submission section, indicating that s/he was not eligible to participate in the study. Respondents were asked to provide the name and link for at least one mHealth app to ensure their eligibility. **Q4-Q9** were demography specific questions, including but not limited to, years of experience, team size, work pattern, etc. **Q10-Q12** aimed to understand the challenges of developing secure mHealth apps. In **Q10**, we proposed a few statements using Likert-scale questions to rate the respondents' agreement to the reported challenges [43]. **Q12** aimed to find out the adopted practices for app development by developers to ensure the security of their apps. **Q13-Q14** aimed to identify the developers’ motivations to develop secure mHealth apps. A few motivating factors were proposed in **Q13** to rate respondents’ agreement. We also provided an **optional question** at the end of our survey to allow respondents to share their comments/feedback.

Pilot and Final Survey: We conducted two pilot studies to validate our questionnaire. First, we specifically distributed the survey to five mHealth apps developers from our contacts and asked them to point out any ambiguities or confusion. Accordingly, clarifications and examples were added. For instance, we asked our respondents to rate their agreement in regards to considering poor security decisions during the development process (SC4) as a challenge. We included “relying on insecure resources, and developer' own assumption" as examples for the provided statement. Second, we posted our survey on social media and received 19 responses with some feedback. Hence, we updated our survey based on the provided comments (e.g., updating/rephrasing some questions etc.). For example, we eliminated two statements (i.e., improper usage of security tools, and using untrusted libraries) from Q10 and include them as an example of insufficient security knowledge (SC1). The survey was designed in English, and took around 15 minutes to complete. Our study is approved by the Human Research Ethics Committee at *The University of Adelaide (H-2019-115)*, as in Appendix E.

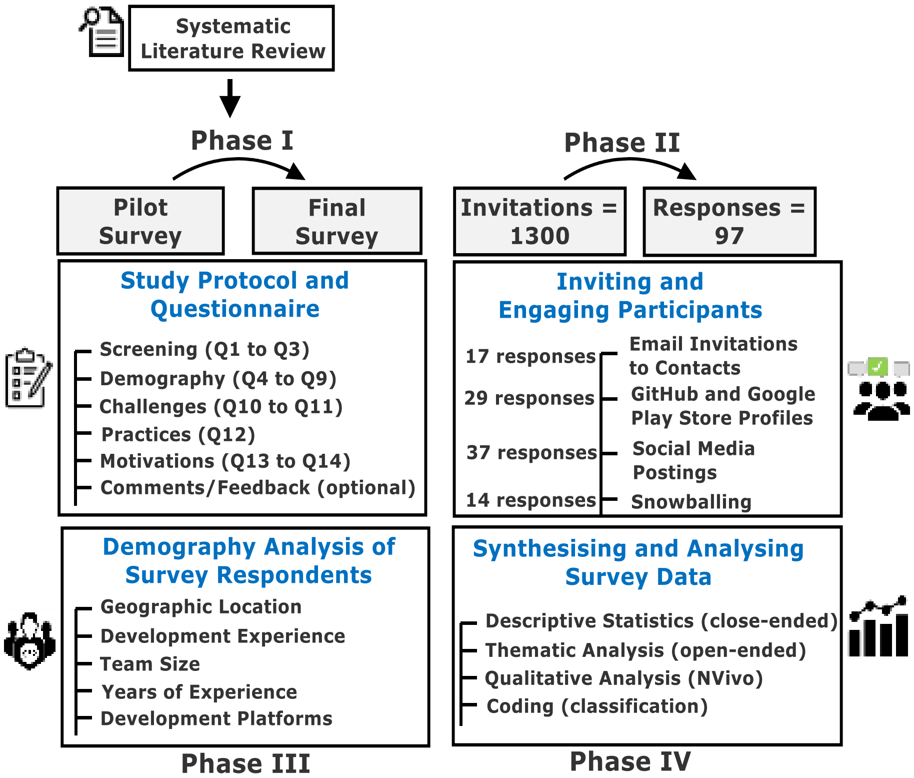


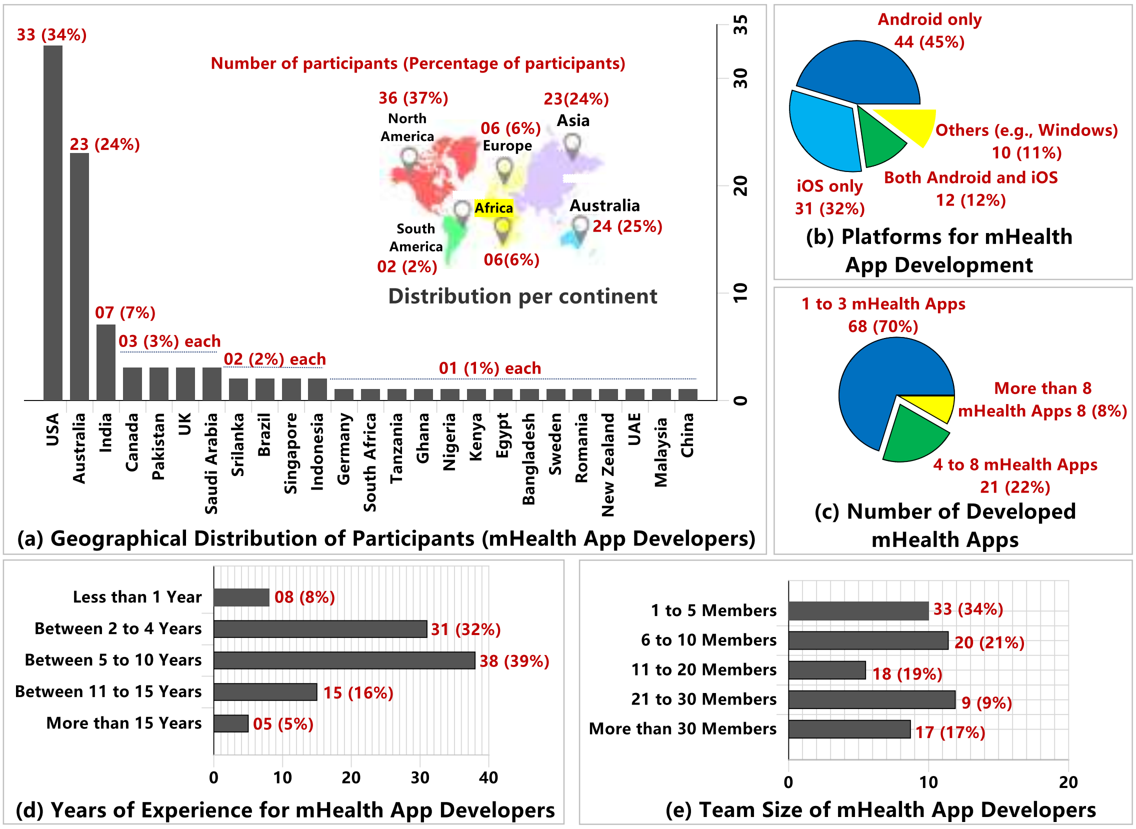
Figure 2.1 An Overview of the Research Method for Developers' Perspectives Study

2.2.2 Phase II – Inviting and Engaging the Participants

Since this study sought specific types of developers (i.e., **Q1-Q3**, Screening in Phase I), we used a different method to ensure that all respondents met our selection criteria. As in Figure 2.1, first, we emailed our contacts who have experience with developing mHealth apps and asked them to participate in the survey. Secondly, we extracted the email addresses of mobile app developers from GitHub and Google Play, which were publicly available in their profiles. We then sent an invitation to over 1300 mobile apps developers. Thirdly, we posted our survey on several mobile app developers' groups on prominent social media platforms (LinkedIn, Facebook, Reddit, etc.). Finally, we followed the snowballing technique to reach more respondents [46]. We obtained 97 valid responses: 37 responses from social media platforms, 29 from GitHub and Google Play users, 17 from personal contacts via email invitations, and 14 through the snowballing technique. The research data were collected between July 2019 and November 2019. Due to the fact that we gathered responses from mHealth apps developers from different parts of the world (i.e., from 25 countries – across six continents), we believe our sample size is representative of this study. The details of the responses from the participants are available in [45].

2.2.3 Phase III – Demography Analysis of Survey Respondents

Once the responses had been obtained, we performed a demography analysis of the survey respondents, which is also referred to as developers' information, as illustrated in Figure 2.2. The demography analysis presented in Figure 2.2 complements the survey responses (**Q1-Q14**) and helped to achieve a fine-grained analysis of the survey results. For example, the platform(s) used for development in Figure 2.2 (b) helped to understand mobile computing platforms most and least preferred by developers to deploy their mHealth apps. Specific mobile platforms may pose different development challenges and encourage developers to adopt different practices for app development [5, 18]. In addition to the details in Figure 2.2, 80% of the respondents had experience as full-time and 20% as part-time developers. All respondents were involved in the development of mHealth apps in various roles, including but not limited to, software engineers, project managers, technical leads, architects, and developers. The full details of the respondents' professional roles are available in [45].



(a) Geographical Distribution of Participants (mHealth App Developers)

(b) Platforms for mHealth App Development

(c) Number of Developed mHealth Apps

(d) Years of Experience for mHealth App Developers

(e) Team Size of mHealth App Developers

Figure 2.2 Demography Analysis of the Survey Respondents (mHealth App Developers)

2.2.4 Phase IV – Synthesising and Analysing Survey Data

We analysed the answers to the close-ended questions (e.g., Likert-scale) using descriptive statistics. For open-ended questions, we used the thematic analysis method [47, 48] to identify any recurring themes in the gathered responses. The thematic analysis supports the extraction of the data and synthesis of the results. We enhanced our analysis by using NVivo software, a popular computer-based tool, to organise and analyse data. The coding was initially done by one person (i.e., the present author) and reviewed and revised (wherever required) by another researcher to avoid potential bias.

2.2.5 Threats to Validity

Threat I – Source and Analysis of Survey Data: We acknowledge that using one source for data collection (i.e., an online survey) may affect our results. We believe that we did not achieve data triangulation, which potentially reduces the accuracy of the findings. Thus, we plan to further extend this study by conducting semi-structured interviews with mHealth app developers to strengthen the current findings. Another possible threat relates to the sampling of respondents. We recruited developers who have experience in developing mHealth apps (as in Figure 2.2, Section 2.2.3). We explained the eligibility characteristics in the survey preamble and all other respondent recruitment documents (e.g., email invitation, post description). We asked the respondents to provide us with a concrete example of mHealth apps which they have developed to ensure their experience and eligibility. Furthermore, since we offered Amazon gift cards to respondents who provided us with eligible and complete responses, it is possible that multiple responses were sent by the same respondent, especially those who have developed more than one mHealth app. In this study, qualitative data collection and analysis may cause irrelevant themes and misinterpretation. To overcome this threat, one person (i.e., the present author) performed the analysis and created initial codes. Another researcher assessed the generated codes, followed by a discussion to confirm the final themes (as in Section 2.2.4).

Threat II – Survey Data Collection and Sample Size: Questionnaire-based research faces the risk of being misunderstood or misinterpreted by respondents. We conducted a pilot survey with a selected pool of respondents to overcome wording and ambiguity issues (as in Figure 2.1). We made some questions compulsory to answer. It was hard to reach respondents who responded earlier to seek their input for the compulsory questions. After sending several emails, we only received a few replies. However, we believe that our study has a convenience sample (i.e., N=97) based on an available pool of mHealth apps developers. All our respondents have developed at least one mHealth app, are geographically diversified, and have different expertise and team size, which reflects the minimum knowledge and expertise to respond.

2.3 End-users' Survey Questionnaire

In this section, we discuss the research method that comprises three phases. Each phase is detailed below as per the illustrations in Figure 2.3. It should be noted that the following research method explains how our studies in Chapter 5, and Chapter 6 were conducted. We also present some of the potential threats that might affect our studies.

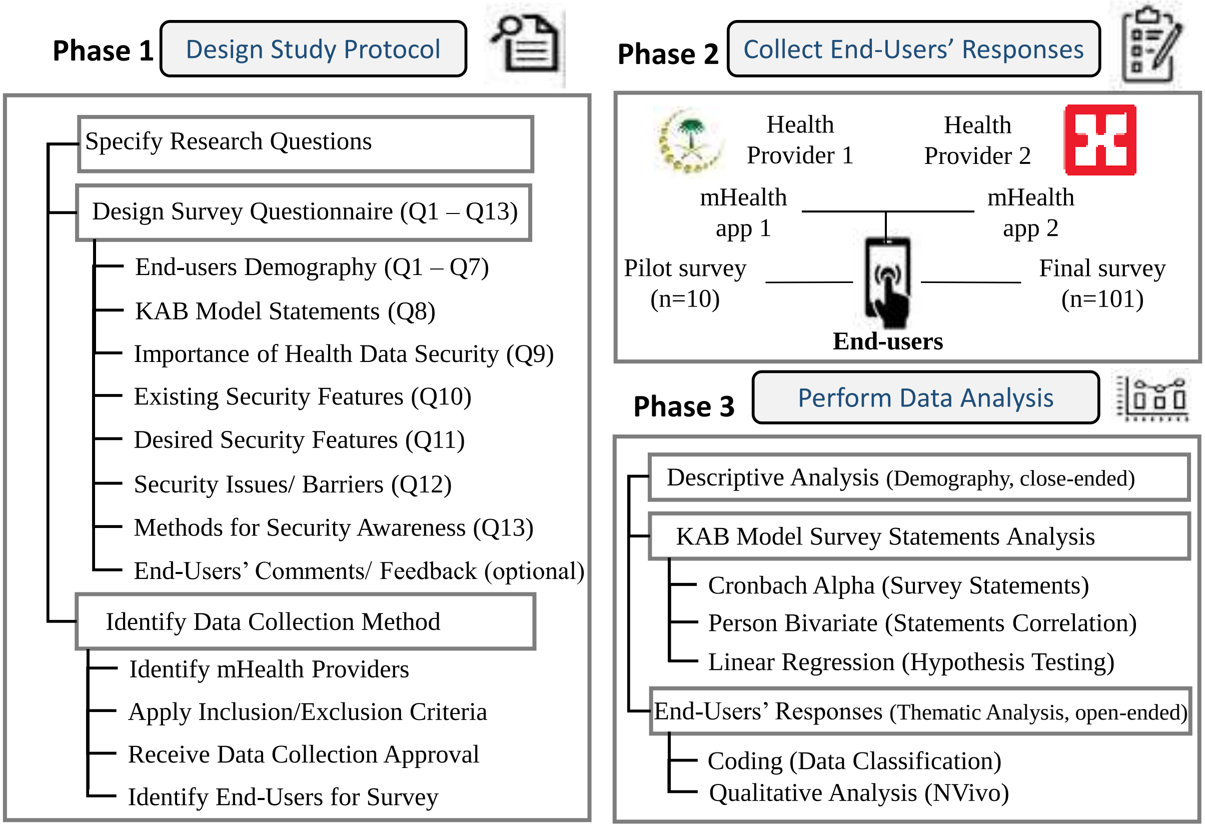

Phase 1
Design Study Protocol
Specify Research Questions
Design Survey Questionnaire (Q1 – Q13)
End-users Demography (Q1 – Q7)
KAB Model Statements (Q8)
Importance of Health Data Security (Q9)
Existing Security Features (Q10)
Desired Security Features (Q11)
Security Issues/ Barriers (Q12)
Methods for Security Awareness (Q13)
End-Users' Comments/ Feedback (optional)
Identify Data Collection Method
Identify mHealth Providers
Apply Inclusion/Exclusion Criteria
Receive Data Collection Approval
Identify End-Users for Survey
Phase 2
Collect End-Users' Responses
Health Provider 1
Health Provider 2
mHealth app 1
mHealth app 2
Pilot survey (n=10)
Final survey (n=101)
End-users
Phase 3
Perform Data Analysis
Descriptive Analysis (Demography, close-ended)
KAB Model Survey Statements Analysis
Cronbach Alpha (Survey Statements)
Person Bivariate (Statements Correlation)
Linear Regression (Hypothesis Testing)
End-Users' Responses (Thematic Analysis, open-ended)
Coding (Data Classification)
Qualitative Analysis (NVivo)

Figure 2.3 Overview of the Research Method for End-Users Perspective Study

2.3.1 Phase 1 – Design Study Protocol

Conducting a rigorous literature review (Chapter 3) enabled us to analyse the collective impact of the existing research, highlighting proposed solutions and their limitations, which helped to specify the research questions and design the survey questionnaire as in Figure 2.3. In the study protocol, we (i) specified the research questions (***RQ6 - RQ10*** outlined in Chapter 1) (ii) designed the survey questionnaire (presented in Appendix C), and (iii) identified the data collection methods. The findings of the literature review and the guidelines provided by Kitchenham and Pfleeger in [44] helped us to design the survey questionnaire that collected end-users' perspectives on mHealth app security. As highlighted in Figure 2.3 the survey (available in Appendix C) contained a total of 14 Questions (**Q1-Q13** and one **optional**) to capture end-users' feedback and recommendations.

Survey Questionnaire for End-users: In order to provide a fine-grained analysis of end-users' feedback and to answer each of the RQs independently, we divided the survey questionnaire into seven different categories. The first series of questions (**Q1-Q7**) record the demography of end-users to help correlate end-users' security knowledge based on factors such as age, level of IT knowledge, and education. **Q8** presents Knowledge, Attitude and Behaviour (KAB) statements regarding the security of mHealth apps (further details are provided in Chapter 5). **Q9** captures users' perspectives about the importance of securing health-critical data, presented as a multi-choice option via a Likert scale (i.e., *very important*, *important*, *neutral*, *not important*, *not important at all*). **Q10-Q11** capture end-users' awareness about the existing security features and security features that are desired as an added value to secure mHealth apps. Specifically, **Q10** presents eight security features identified from the literature using a Likert-scale with five options for each feature (i.e., *always*, *sometimes*, *rarely*, *never*, *I don't know*). **Q11** is an open-ended question that asks end-users to suggest the security features that may be missing from the existing apps but are highly desired. **Q12** is an open-ended question that aimed to explore the security barriers experienced by end-users when using mHealth apps. **Q13** is an open-ended question that aimed to find out the methods used to make end-users aware of the security of mHealth apps. An optional question is also added at the end of our survey to allow respondents to share their comments and/or feedback.

Selection of mHealth apps: To identify which mHealth apps to investigate and how to collect data for the study, we searched in the two major app repositories (i.e., Google Play by Android and App Store by iOS) to find out what mHealth apps are available and who provides them. We needed to collaborate with mHealth app providers that (i) have functional mHealth apps and (ii) could provide us with a survey of their end-users (medical professionals, patients, clinical technicians, etc.). We were interested in the type of apps that can be used in the clinical setting by enabling their users to access a wide range of services (e.g., reviewing medical records, viewing scanned images and lab results, etc.). We limited our search for mHealth apps, provided by approved Saudi Arabian mHealth providers. Saudi Arabia can be considered one of the fastest developing countries in the Middle East, to adopt mHealth apps. Based on our search of the available mHealth apps provided by health providers, we found 16 mHealth apps. We excluded four health providers since their apps had a low number of downloads or did not interact with end-users for their health data. We contacted 12 health providers to seek their approval to collect data on-site. In December 2019, we received approval from two health providers[2], namely (i) *King Fahad Medical City* – KFMC (with the iKFMC app, launched in 2017, which has more than 50,000 downloads, 420 reviewers, and a user rating of **3.8**), and (ii) the Dr Sulaiman Al Habib Medical Group – HMG (with the Dr. Sulaiman Alhabib app, launched in 2016, which has more than 100,000 downloads, 9034 reviewers, and a user rating of **4.4**).

2.3.2 Phase 2 – Collect End-users' Responses

To collect end-users' responses, the two mHealth providers (KFMC, HMG) were purposefully chosen because they provide mHealth apps that allow their users to access a wide range of services such as creating, storing, and sharing medical records, viewing scanned images, lab results, and automating their clinical practices. The first author personally visited both mHealth providers during January and February 2020 to carry out the study and collect data. The collection of data occurred through meeting end-users in person during their visits to the outpatient clinics of the two health providers. The end-users willing to participate in the survey were provided with the option to either take a hard copy to be filled out or scan a QR code with their devices to access the online version of the survey. The survey preamble briefly described the purpose of the study, and who would be eligible to participate. To maintain the reliability of the collected responses, we focused on ensuring that potential respondents were: 1) briefed about the survey and that one researcher was present at all times to clarify any issues, 2) allowed to exit the survey at any time they desired, and 3) were experienced in using the provided mHealth apps. As in Figure 2.3, first, we conducted a pilot study with approximately 10% of the

[2] King Fahad Medical City (KFMC) https://www.kfmc.med.sa/EN/Pages/Home.aspx
mHealth app: *iKFMCApp:* https://play.google.com/store/apps/details?id=sa.med.kfmc&hl=en
Dr. Sulaiman Al Habib Medical Group (HMG) https://hmg.com/en/pages/home.aspx
mHealth app: Dr. Sulaiman Alhabib App: https://apps.apple.com/ae/app/dr-sulaiman-alhabib/id733503978

respondent population which helped us to finalise the survey questionnaire. Accordingly, we provided further explanation within the given statements and removed some technical terms (e.g., SSH for secure data communication) that end-users can find confusing. For example, we clarified the meaning of third parties in the statement "I get informed when my health data, which have been collected by mHealth apps, are being shared with third parties" in Q8. We added "other health providers, clinics as examples of third parties. Incomplete responses were removed, and thus, a total of 101 accurate and acceptable responses (referred to as **R1** to **R101**) from the end-users were collected on-site at KFMC and HMG. The survey took approximately 10 minutes to complete.

It is worth mentioning that all end-users that we surveyed and both the mHealth providers were based in Saudi Arabia, thus limiting the geo-distribution of survey participants and could impact the study findings. Some travel restrictions globally, during the said time period, also limited our planned on-site data collection from more countries. Extended work is in progress on designing and deploying a web-based survey and a case study to seek feedback from geographically diverse end-users and their healthcare providers.

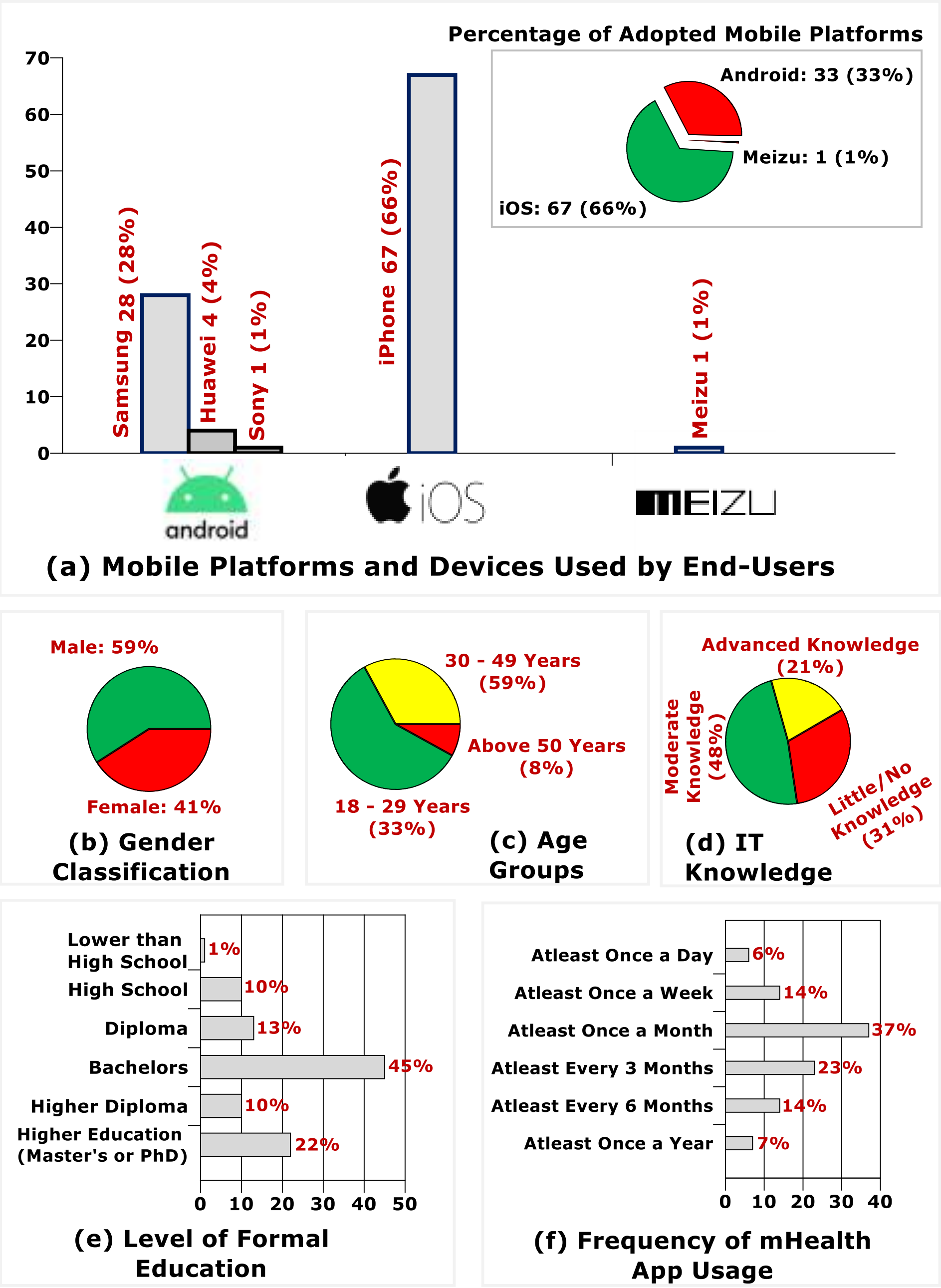


Figure 2.4 Demographic Details of mHealth Apps End-Users (Sample Size =101)

2.3.3 Phase 3 – Perform Data Analysis

In the last phase of the methodology, we performed data analysis based on end-users' responses as in Figure 2.3. We used SPSS (Statistical Package for Social Science) version 27 (IBM) for the quantitative analysis of data. A **descriptive analysis** was conducted to report the respondents' demographic data as well as the obtained responses for **Q9**, and **Q10**. As in Figure 2.4 above, the demography analysis included factors such as mobile platforms, gender classification, age group, and level of end-users' IT knowledge. The respondents' demographic information was used to contextualize the responses that complement security awareness for a specific group of users. For example, we were able to investigate if the level of formal education, and IT knowledge had an impact on the security awareness of end-users. To determine the security awareness regarding the existing security features for a specific group of users, we conducted the **Independent-Sample T-test** for gender since we were comparing two independent populations (i.e., male and female), and the **Kruskall-Wallis H test** for more than two independent populations (e.g., IT knowledge level, age group, etc.) followed by a post hoc test to examine the significance of differences in the mean scores for the specific group of users. It is worth mentioning that the indicated statistical tests require passing certain assumptions before running each test; and hence, the assumptions have been checked to ensure the reliability of the results. For each demographic data, we tested the null hypothesis (i.e., *H0: there is no significant difference*) against the alternative hypothesis (i.e., *H1: there is a significant difference*), whereas *μ1, μ2, …, μk* refers to population means. A **descriptive analysis**, along with mean and Standard Deviation (SD) were performed to report the respondents' demographic data and the survey responses. We calculated the **Cronbach Alpha** to measure the reliability and internal consistency of **Q8** survey statements. We performed two **Linear Regression tests** to test the research hypotheses (more details related to this part are provided in Chapter 5).

For qualitative data, a **thematic analysis** method [47, 48] was performed to analyse the textual responses of end-users (i.e., **Q11 - Q13**) corresponding to ***RQ9***, ***RQ10***, and the second part of ***RQ8***. To further enhance the analysis, NVivo was used to organise and analyse the data. The initial coding was done by one person (i.e., the present author) and reviewed and revised (wherever required) by another researcher to avoid potential bias. We mainly followed the five steps of the conceptualized thematic analysis method. First, we reviewed and examined the provided responses to determine the parts that were relevant to each of the research questions indicated in Chapter 1. Second, we generated the initial codes for each research question. Third, we tried to combine different initial codes generated from the second step into potential themes. Fourth, we reviewed and refined the identified themes by checking them against each other to understand what themes had to be merged with others or dropped. Lastly, we assessed the trustworthiness of each main theme and created a name for each of them. Figure 2.5 demonstrates an example of the qualitative data analysis that led to our findings. For example, as in Figure 2.5, in the context of ***RQ9*** (end-users' understanding of existing security features and the desired security features), one participant's response was, *'Use of finger print is helpful to login but sometimes verification text arrives too late … '*. This response helped us to identify that biometric-based 2FA, which follows an SMS activation code, is a desired security feature by end-users; however, any other issues that delay the reception of the activation code could restrict the user from logging in to the app. Figure 2.5 also highlights that end-users' responses related to app usability such as*'… using distinct colours and sound notifications will help'* were discarded from the analysis to strictly focus on the security aspects of the apps.

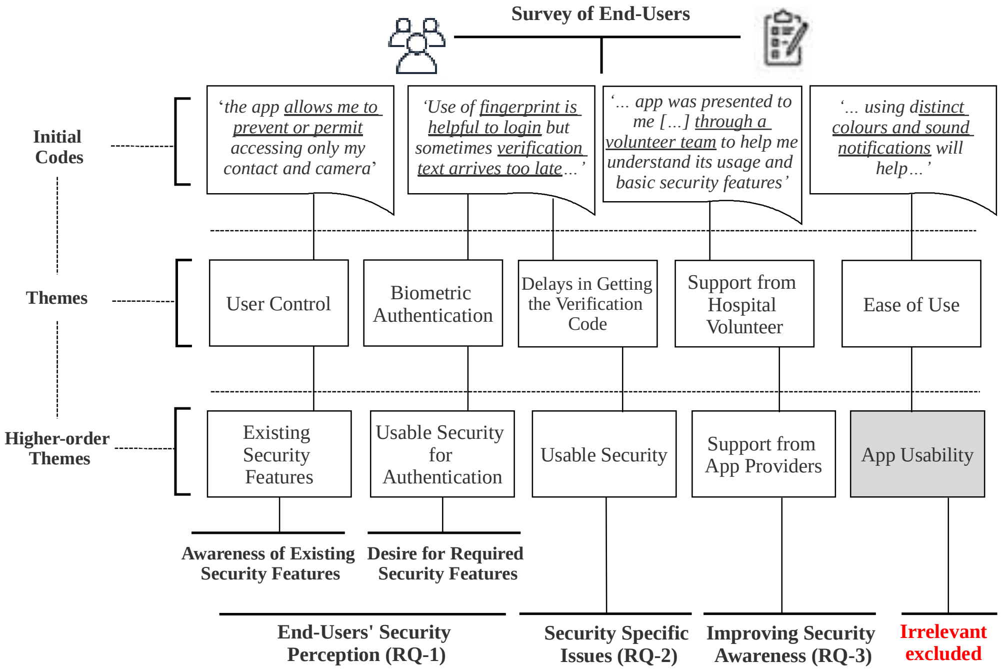

Survey of End-Users
Initial Codes
Themes
Higher-order Themes
'the app allows me to prevent or permit accessing only my contact and camera'
'Use of fingerprint is helpful to login but sometimes verification text arrives too late…'
'… app was presented to me […] through a volunteer team to help me understand its usage and basic security features'
'… using distinct colours and sound notifications will help…'
User Control
Biometric Authentication
Delays in Getting the Verification Code
Support from Hospital Volunteer
Ease of Use
Existing Security Features
Usable Security for Authentication
Usable Security
Support from App Providers
App Usability
Awareness of Existing Security Features
Desire for Required Security Features
End-Users' Security Perception (RQ-1)
Security Specific Issues (RQ-2)
Improving Security Awareness (RQ-3)
Irrelevant excluded

Figure 2.5 The Steps of Applying Thematic Analysis to Qualitative Data

Ethics Approvals: Both mHealth providers granted approval for on-site data collection through their Institutional Review Board (KFMC approval number: *19-462E*, HMG approval number: *HAP-01-R-082*). Our study was also approved by the Human Research Ethics Committee at the *University of Adelaide (H-2019-165)*. Further details of the research method, and statistical data analysis are available in [49]. All ethics approvals documents are presented in Appendix E.

2.3.4 Threats to Validity

We now discuss some of the threats to the validity of this study. There are three types (i.e., internal, construct, and external) validity threats to be discussed below.

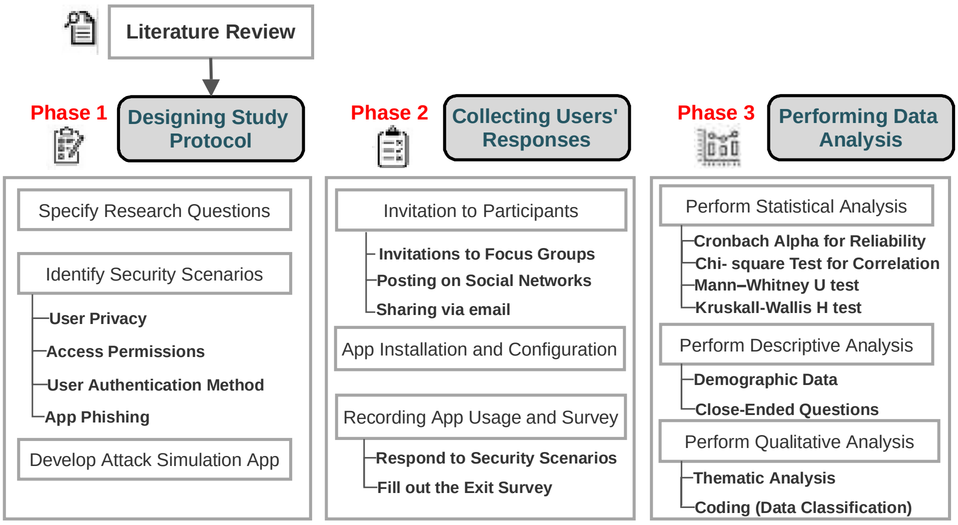
Internal validity refers to the extent to which the observed results were from a reliable population. The proposed study collected data by means of surveying end-users of mHealth apps. Relying solely on the end-user survey for data collection and lack of triangulation could have impacted the reliability of the findings. Another possible threat relates to the participants' subjective viewpoints, which could have been misinterpreted when analysing the qualitative data. To overcome this threat, the initial coding of the data was done by one person (i.e., the present author) followed by the evaluation and finalization of the codes by another researcher). Figure 2.5 in Section 2.3.3 presents an example of data coding as an attempt to minimize this threat.

Construct validity refers to the extent to which the used instrument measures what it is supposed to measure. Employing a suitable instrument for data collection and synthesis can threaten the validity of study results. We believe collecting data about end-user' behaviour could affect the findings (Chapter 5 in particular). Our study relied on survey-driven feedback as self-reported knowledge, attitude, and behaviour of end-users, which involves potential human bias in reporting. We tried to minimize this bias with the use of the Knowledge, Attitude, and Behaviour (KAB) [50] and Human Aspect Information Security-Questionnaire (HAIS-Q) [39, 51] models. Based on the outlined hypothesis (Phase 3, Figure 2.3) and their validation (Section 5.4), respondents' knowledge had not influenced their behaviour towards mHealth security. We consider such correlation as an indication of fair responses by participants. To further ensure unbiased data collection, we designed an initial version and conducted a pilot survey (engaging 10 participants, Figure 2.3) based on the literature review and then analysed the mHealth apps that were deployed on-site by our collaborators (KFMC and HMG). The pilot survey helped us to revise the survey questionnaire by eliminating any bias or confusion in the survey statements. The respondents who participated in the pilot survey suggested clarifying adjustable security settings in the sixth statement of **Q9**. Thus, we updated the relevant part of the survey with the addition of a controlling app permissions option, as in Figure 2.3. Furthermore, the initial questionnaire and pilot survey were validated by other members within the research group. As a result, some questions were slightly modified to avoid confusion. For instance, a statement in **Q8** related to encrypting health data during transmission and storing was removed because it was not actionable by the respondents. Due to the requirements of data privacy and ethics approval, the survey was possible only within the premises of our collaborating mHealth providers. This limited our efforts to engage more end-users with diverse backgrounds and different app usage, beyond two healthcare providers. The end-user survey could not accommodate the other means of data collection such as users' interviews and focus groups interactions for fine-grained collection and analysis of security awareness.

External validity refers to applying the generalization of the study results. As per the statistics for the number of downloads, according to the Google Play store (App Store does not show publicly the number of downloads; it can be viewed by app providers only), each app (i.e., KFMC app, HMG app) was downloaded by more than 10,000 end-users. In comparison to on-site data collection, a web-based survey with geographically distributed end-users can increase the participation (number of participants) and diversity of data collection (different apps from across the globe). The findings of our study are based on end-users' views from two health providers in Saudi Arabia; hence, our results may not be generalizable due to geographical restrictions. Furthermore, our respondents might be influenced by the assigned policies and regulations when following practices in the examined mHealth providers in Saudi Arabia. Such a policy could allow sharing end-user's health data with law enforcement agencies without end-user's consent, or sharing health data with another health professional for consultation, especially when the patient is in an emergency and unconscious. Therefore, we plan to further extend this research by collaborating with other mHealth providers globally.

2.4 Simulation-Based Attack

In this section, we discuss the research method that we followed to measure the security awareness of end-users of mHealth apps through a simulation-based attack (Chapter 7). The adopted method comprises three phases, each detailed below, as per the illustrations in Figure 2.6.



Literature Review
Phase 1
Designing Study Protocol
Phase 2
Collecting Users' Responses
Phase 3
Performing Data Analysis
Specify Research Questions
Identify Security Scenarios
User Privacy
Access Permissions
User Authentication Method
App Phishing
Develop Attack Simulation App
Invitation to Participants
Invitations to Focus Groups
Posting on Social Networks
Sharing via email
App Installation and Configuration
Recording App Usage and Survey
Respond to Security Scenarios
Fill out the Exit Survey
Perform Statistical Analysis
Cronbach Alpha for Reliability
Chi- square Test for Correlation
Mann–Whitney U test
Kruskall-Wallis H test
Perform Descriptive Analysis
Demographic Data
Close-Ended Questions
Perform Qualitative Analysis
Thematic Analysis
Coding (Data Classification)

Figure 2.6 Overview of Research Method for Attack Simulation Approach Study

2.4.1 Phase 1 – Design Study Protocol

Our literature review in Section 3.2 helped us understand state-of-the-art on end-users security issues, concerns, and preferences when using mHealth apps. In addition, we reviewed the literature to identify the existing methods to measure end-users security awareness when using mobile apps (Section 3.3). Consequently, we understand and analyse the impact of the current research, highlighting proposed solutions and their limitations, specifying the research questions, and designing our study as in Figure 2.6. In the study protocol, we (i) specified the research questions (***RQ12,*** and ***RQ13*** outlined in Section 1.1) (ii) identified the security scenarios that we planned to investigate, as in Table 2.1, and (iii) developed the simulation app. We investigated three major security threats, including user privacy and app permissions, authentication, and application phishing. It should be noted that each major security threat has a few potential security threats and at least one attack scenario, as highlighted in Table 2.1. We also gave the participants the option of reporting any security threats that they found and their interest in receiving security advice or training. Furthermore, we concluded our experiment with an open-ended question to capture end-users' thoughts in regards to the reasons behind paying attention to app permissions and the impact of giving an app more access permissions.

Identification of Security Scenarios: Studies such as [23, 24, 40, 52, 53] examined end-users' views about the security of mHealth apps. The surveyed participants agreed that mHealth apps need to implement security countermeasures that ensure confidentiality, availability, and integrity of health-critical data. However, there is a lack of evidence based on what participants' reactions are in real scenarios. Studies such as [54-59] conducted experimental research to measure the security behaviours of end-users of mobile apps when they face certain security challenges (e.g., phishing attacks, app permissions). These studies have inspired our research and significantly helped us to identify four security threats and eight security scenarios to be examined as illustrated in Table 2.1. To further understand the participants' reactions to these security threats, we included an option to report the security issues that they may notice. In addition, we asked our participants in case they want to learn about security which can help us to plan further research. This study is approved by the Human Research Ethics Committee at the *University of Adelaide (H-2021-106).* It should be noted that due to the conditional ethics approval, we omitted some security scenarios (e.g., requesting unnecessary information from participants, investigating password strength and updating passwords) to ensure participants' anonymity, avoid collecting sensitive data such as passwords.

Table 2.1 The Investigated Security Threats and Scenarios in the Simulation-based Attack Study

Major security threats	**Minor sub-security threats (Potential Security Threat)**	**Example (Scenarios/use-cases)**
A. User Privacy and Permissions	1. Reading privacy policy	• Show privacy policy to end-users to investigate the time spent to read it.
	2. Requesting permission to access device resources (e.g., user location, contacts, photos, microphone, camera, data of other apps)	• Request access permissions that are not mandatory for the app. The given permission for users can be either accept, or deny.
B. Authentication	3. Selecting secure authentication methods (e.g., none, PIN, 2FA, etc.).	• Provide a few options for authentication to investigate end-users' preferences.
C. Application Phishing	4. Pop-up window that requests users to share their private information.	• Show a pop-up window to request information from end-users giving them the options to allow pop-ups, or discard pop-ups.

D. Feedback and reporting	5. Reporting security issues to developers.	• Ask participants if they want to contact developers to report any security issues.
	6. Understanding users interest in security education and training.	• Provide a signup option to receive frequent emails on secure mobile app usage.

Simulation Mobile App: We developed a fitness app called "Workout" to convince participants to be a part of the study. Due to the time limit that we had to complete this research, we made the app (.APK file) downloadable directly for our storage instead of uploading it to apps stores. In fact, some participants were in doubt about installing the simulation app on their devices. The .APK file is available in [60]. Thus, we assured them that this is a part of a research study that we received ethical approval from concerned authorities and institutes to conduct this research and that the collected data will be anonymous and will be used solely for research purposes. We developed the simulation app to attract the participants by providing useful content such as workout plans, specific muscles exercise, etc. As an appreciation of our participants' time, we gave full access to the app (i.e., no subscription fees, no ads within the app) by removing all things that related to the study and make available on the app markets. A promotion code was given to all participants to use the app for free.

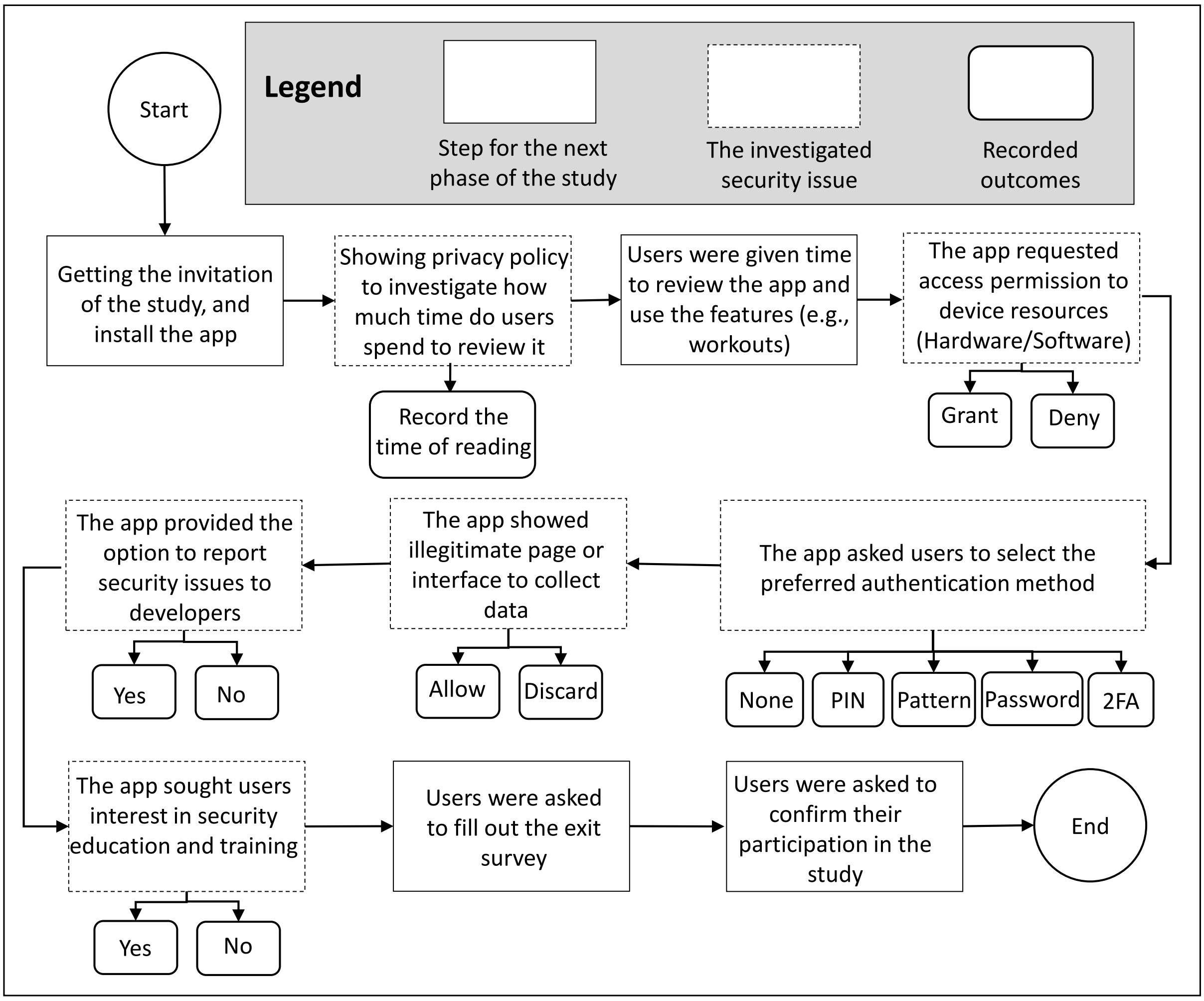
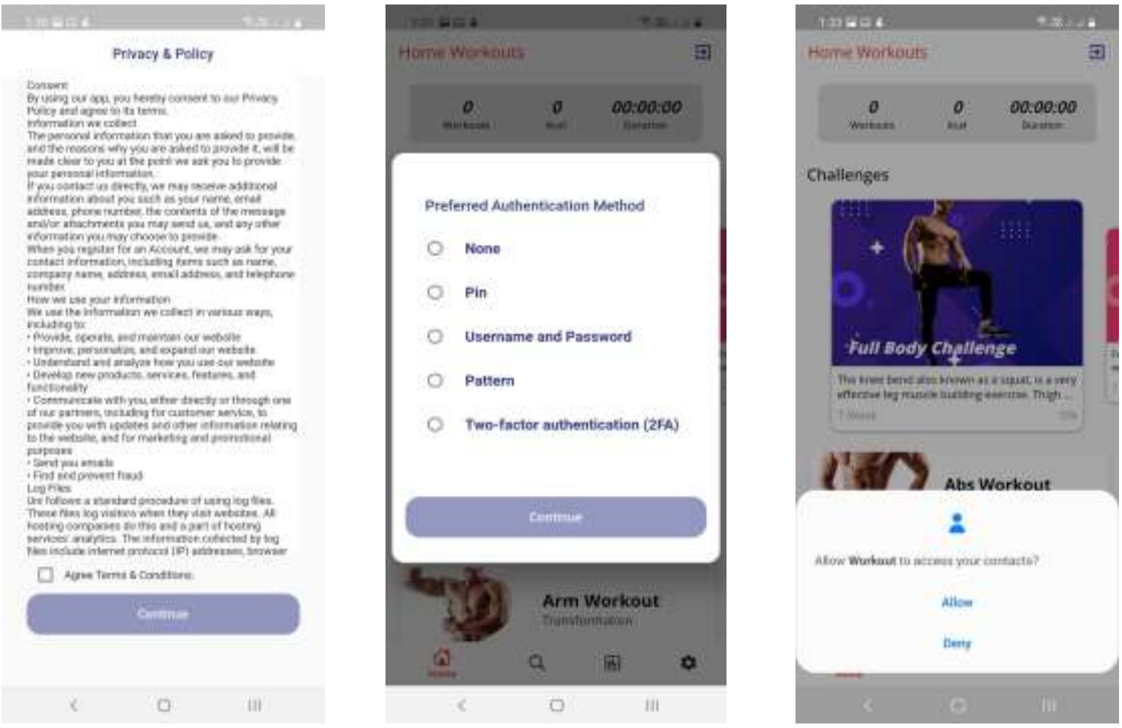

Start
Legend
Step for the next phase of the study
The investigated security issue
Recorded outcomes
Getting the invitation of the study, and install the app
Showing privacy policy to investigate how much time do users spend to review it
Record the time of reading
Users were given time to review the app and use the features (e.g., workouts)
The app requested access permission to device resources (Hardware/Software)
Grant
Deny
The app asked users to select the preferred authentication method
None
PIN
Pattern
Password
2FA
The app showed illegitimate page or interface to collect data
Allow
Discard
The app provided the option to report security issues to developers
Yes
No
The app sought users interest in security education and training
Yes
No
Users were asked to fill out the exit survey
Users were asked to confirm their participation in the study
End

Figure 2.7 Flowchart of the Study Procedure

2.4.2 Phase 2 – Collect End-users' Responses

Recruitment for Participants: We targeted anyone who uses an Android device since our simulation app is only compatible with Android OS. We advertised for our study by posting our study invitation on social networks (e.g., Twitter, Facebook, LinkedIn, Reddit, WhatsApp groups, etc.) to recruit participants. Our app was available to download by visiting a designed webpage that also include instructions to involve in the study. Participant has to be at least 18-year-old to engage in the study. We were able to monitor participants' reactions from the moment they install the app and we recorded their security reactions. Participants faced many challenges related to the security aspects of mobile health apps, as illustrated in Table 2.1. Figure 2.8 shows six examples (screenshots) of the research activities that our participants faced. Additional screenshots for our simulation app are available in [60]. In the end, we provided an exit survey to collect demographic data and an open-ended question to allow them to share their thoughts. It should be noted that we carried out pilot testing for our study with at least 10% of the participants to ensure reliability and validity. Participants were given the option to withdraw their data during the study by simply deleting the app. As a result, their responses would be considered incomplete and hence excluded from further analysis. After removing incomplete responses (i.e., we consider the response is complete when the participants went through all security scenarios which we are investigating, and filled out the exit survey), we were able to collect data from 105 participants (referred to as **P1** to **P105**). The research data for this study were collected between July 2021 and August 2021. The collected data along with the exit survey questions are available in [60]



Privacy & Policy

Consent
By using our app, you hereby consent to our Privacy Policy and agree to its terms.
Information we collect
The personal information that you are asked to provide, and the reasons why you are asked to provide it, will be made clear to you at the point we ask you to provide your personal information.
If you contact us directly, we may receive additional information about you such as your name, email address, phone number, the contents of the message and/or attachments you may send us, and any other information you may choose to provide.
When you register for an Account, we may ask for your contact information, including items such as name, company name, address, email address, and telephone number.
How we use your information
We use the information we collect in various ways, including to:
• Provide, operate, and maintain our website
• Improve, personalize, and expand our website
• Understand and analyze how you use our website
• Develop new products, services, features, and functionality
• Communicate with you, either directly or through one of our partners, including for customer service, to provide you with updates and other information relating to the website, and for marketing and promotional purposes
• Send you emails
• Find and prevent fraud
Log Files
Urs follows a standard procedure of using log files. These files log visitors when they visit websites. All hosting companies do this and a part of hosting services' analytics. The information collected by log files include internet protocol (IP) addresses, browser

□ Agree Terms & Conditions

Continue

(a) Privacy Policy for our simulation app

Preferred Authentication Method

○ None

○ Pin

○ Username and Password

○ Pattern

○ Two-factor authentication (2FA)

Continue

(b) Selecting the preferred authentication method

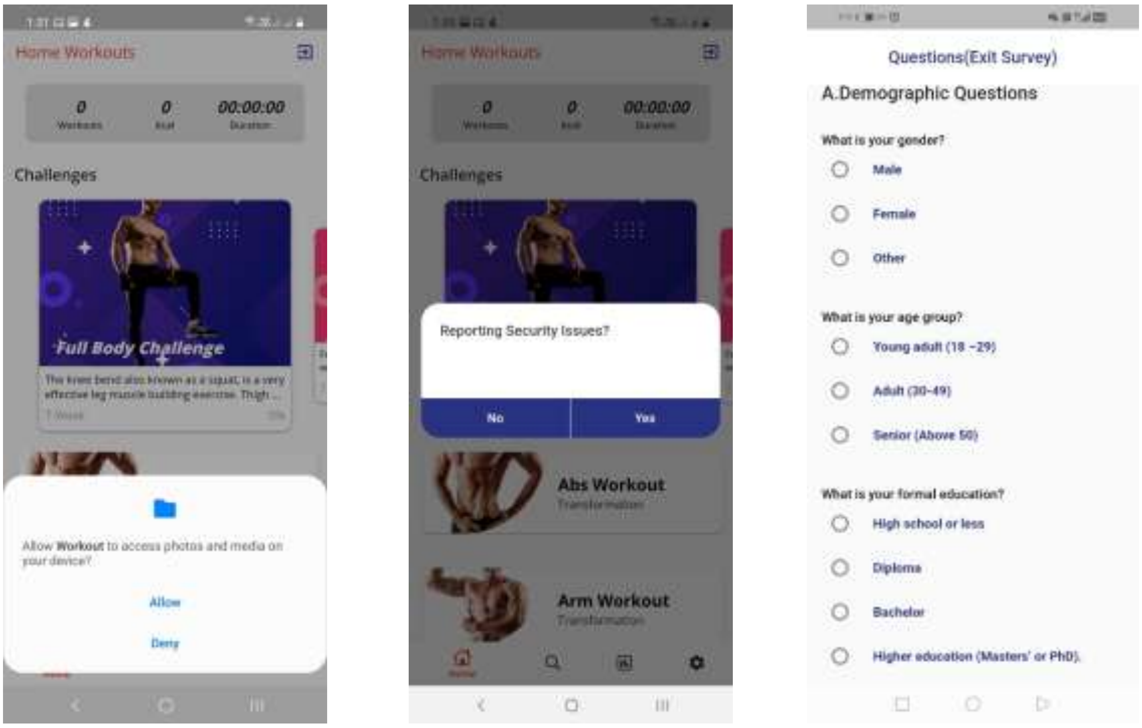
Allow **Workout** to access your contacts?

Allow

Deny

Home Workouts
0
Workouts
0
Kcal
00:00:00
Duration
Challenges
Full Body Challenge
The knee bend also known as a squat, is a very effective leg muscle building exercise. Thigh ...
Abs Workout

(c) Example of requesting access permission from participants



The knee bend also known as a squat, is a very effective leg muscle building exercise. Thigh ...

Allow **Workout** to access photos and media on your device?

Reporting Security Issues?

Questions(Exit Survey)

A.Demographic Questions

What is your gender?

○ Male

○ Female

○ Other

What is your age group?

○ Young adult (18 –29)

○ Adult (30–49)

○ Senior (Above 50)

What is your formal education?

○ High school or less

○ Diploma

○ Bachelor

○ Higher education (Masters' or PhD).

(d) Example of requesting access permission from participants

(e) Reporting security issue about the simulation app

(e) Exit survey for the simulation app

Figure 2.8 Examples of Research Activities for Simulation-based Attack Study

Participants' characteristics: our study engaged participants from various countries (i.e., 14 countries, five continents), and with different age groups (participants should be at least 18 years old). Furthermore, our participants were having various educational backgrounds and different IT knowledge. The demography analysis presented in Figure 2.9 complements the exit survey responses (**Q1**-**Q6**), available in Appendix E, and helps us with a fine-grained analysis of the study results. For example, the analysis helped us to understand the difference in male and female reactions to access permissions. We were able to recruit 105 Android devices users. Figure 2.9 (a) presents the geographical distribution of our study participants. 64% were male, and 36% were female as in Figure 2.9 (b). As in Figure 2.9 (c), 45% were aged 18 – 29, 50% were aged 30 – 49, and only 5% of our population were above 50. A bachelor's degree was the most reported level of formal education for our respondents (i.e., 50%). 26% were postgraduate level, 13% had a diploma, and 10% were high school educated or less, as in Figure 2.9 (d). Regarding the respondents' IT knowledge, 46% reported that they have little or no knowledge, 40% considered themselves as having moderate knowledge, and only 14% had advanced knowledge, as in Figure 2.9 (e).

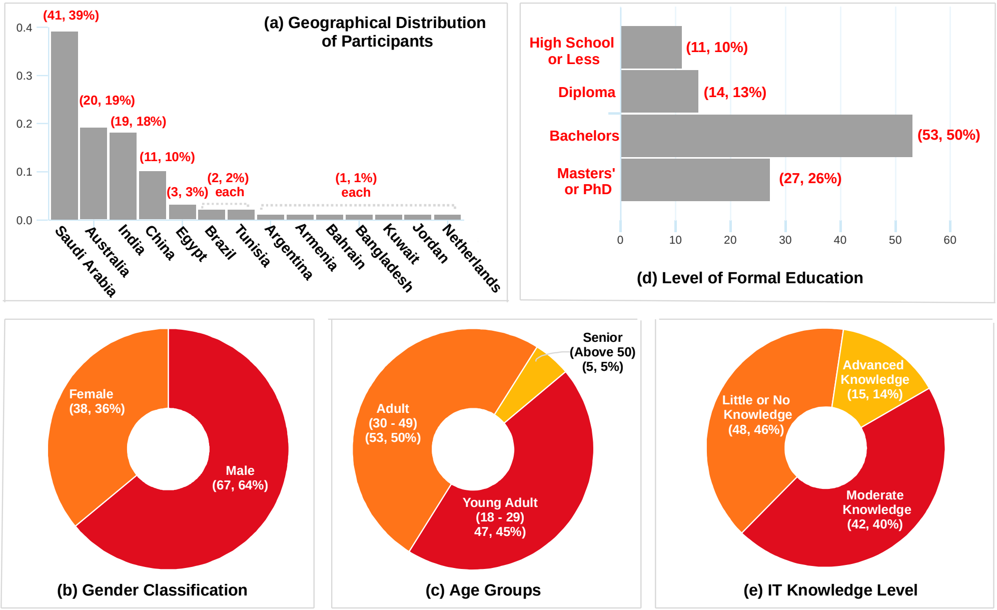


Figure 2.9 Demographic Details of the Participants in the Attack-Simulation Study (Sample Size =105)

2.4.3 Phase 3 – Perform Data Analysis

For this study, we collected quantitative and qualitative data that help us to answer the outlined RQs. Based on the nature of the data and the purpose of the analysis, we performed three techniques. Each technique is detailed below as per the illustrations in Figure 2.6.

Statistical analysis: SPSS version 28 (a popular data analysis software) was used in this technique. To measure the reliability and internal consistency of the dichotomous study items (i.e., permission requests), we calculated the **Cronbach Alpha** to ensure that we meet the minimum acceptable coefficient value (i.e., ≥ 0.7) [61]. We also evaluated the correlation between the permission requests responses using the **Chi-square test** [62]. This test helped us to understand the correlation (i.e., strength and direction of association) between the permission requests items. Furthermore, we used statistical significance to compare our participants' reactions to the requested access permissions among multiple groups of end-users. **Mann–Whitney U test** was performed to compare the gender group since we have two independent samples (i.e., male and female) [63]. The **Kruskall-Wallis H test** was performed to compare the participants' reactions for more than two independent populations (e.g., IT knowledge level, age group, etc.) followed by a post hoc test to examine the significance of differences in the mean scores for the specific group of users [64, 65]. It is worth mentioning that the indicated statistical tests require passing certain assumptions before running each test; and hence, the assumptions have been checked to ensure the reliability of the results. For each demographic data, we tested the null hypothesis (i.e., *H0: there is no significant difference*) against the alternative hypothesis (i.e., *H1: there is a significant difference*), whereas *μ1, μ2, …, μk* refers to population means.

Descriptive analysis: We reported the participants' demographic data by using **descriptive analysis** as presented in Figure 2.9. We also used this technique to report the participants' reactions when we asked them to make certain security decisions during using the simulation app (e.g., requesting the user to select the preferred authentication method, requesting access to device storage, etc.).

Qualitative analysis: For the open-ended question, we used the **thematic analysis method** [47] (as discussed in Section 2.3.3) to identify the reasons that end-users reported about paying attention to the requested access permissions. The thematic analysis supports extracting the data and synthesizing the results. We used NVivo software, a popular computer-based tool, to organise and analyse data. It should be noted that one person (i.e., the present author) conducted the qualitative analysis, which was then assessed by another researcher to avoid biases. Further details about the methodology, statistical data analysis, and ethics approval are in [60].

2.4.4 Threats to Validity

We now discuss some threats to the validity that represent potential limitations that might impact the finding of this study. Validity threats are the results of certain assumptions or constraints that need to be highlighted and ideally eliminated as part of future research.

Internal validity refers to the factors that could have impacted data collection and analysis processes negatively. The study collected data through a simulation app that we developed. It presented some real-life security scenarios that any end-users face during mobile apps usage. However, the study findings might get affected since we had to explicitly indicate to the participants that we were investigating their security awareness. Initially, we planned to hide the aim of the study by mentioning that we are going to investigate participants' habits and behaviours towards mHealth apps. Yet, due to the limited disclosure of the study aim, we were not able to get ethical approval. Indeed, the application of our study was elevated to a high-risk review, and it took so many reviews until we addressed the concerns of the ethics committee (i.e., explaining the aim of the study to participants in advance). Another threat can be analysing qualitative data of the exit survey, which may lead to misinterpretation of participants' responses. To overcome this threat, the initial coding of the data was done by one person (i.e., the present author) followed by the evaluation and finalization of the codes by another researcher).

Construct validity refers to the extent to which the used instrument measures what is supposed to be measured. Due to the limited time to finish the study, the app was available to download from our storage. Thus, we found collecting data was a bit challenging since we were trying to convince participants to download an app using an .APK file without referring to the apps market. Participants were sceptical because most of them received a warning message from their devices to not download the app as it could be malicious. Our study could also be impacted by the limited security scenarios that we already measured. Some security scenarios (e.g., password strength, password changing habits) were questionable by the ethics committee; hence, we had to omit them to get the study done. The other limitation is that our simulation app is only compatible with Android devices. The given time to finish the research has limited us to configure the app with iOS devices.

External validity refers to applying the generalization of the study results. The findings of our study cannot be generalized since we have a limited number of some categories (e.g., a few participants above the age of 50). Thus, we plan to further extend this study by including more security scenarios, other research methods (e.g., semi-structured interviews, think aloud, etc.), and more open-ended questions. In addition, we plan to reach a large number of participants geographically distributed (i.e., include participants with spoken languages other than English). This would help us to increase the number of participants and diversity of data collection.

Chapter 3

Literature Reviews

Related publication:

Section 3.1 in this chapter is based on our paper titled "Challenges in Developing Secure Mobile Health Applications: Systematic Review" [43] which was published in JMIR mHealth and uHealth.

mHealth apps have gained significant popularity over the last few years due to their tremendous benefits such as lowering healthcare costs and increasing patient awareness. However, the sensitivity of healthcare data makes the security of mHealth apps a serious concern. It is important to explore the security aspects of mHealth apps from both developers' and end-users perspectives. This chapter aims to identify and explore the security challenges that prevent the developers of mHealth apps to implement security during the development process, understand end-users security perceptions towards using mHealth apps, and identify the existing approaches to measure end-users' security behaviour when they face security threats while using mHealth apps. The SLR results revealed nine challenges that influence the implementation of the security of mHealth apps during SDLC such as lack of security guidelines and regulations for developing secure mHealth apps, and developers' lack of knowledge and expertise for secure mHealth app development. This chapter reported the security perceptions of end-users when using mHealth apps, reported the security issues that end-users of mHealth apps are concerned about, and the security measures that increase end-users' confidence level when using mHealth apps. Furthermore, this chapter identified the methods used to measure the security awareness of the end-users of mobile apps. This chapter is organized as follows. Section 3.1 presents the SLR findings for RQ1: What are the reported challenges in literature that developers of mHealth apps face with respect to implementing security? Section 3.2 addresses RQ5: What are the security knowledge and perceptions of end-users about using mHealth apps, which have been reported in the literature? Section 3.3 addresses RQ11: What are the security characteristics in the context of mHealth apps that we need to measure? And how they can be measured?

3.1 Developers' Views of Security of mHealth Apps (RQ1)

3.1.1 Introduction

The use of mobile applications (apps) in healthcare has gained widespread adoption [15, 66]. The lack of health professionals, especially in rural areas, is an excellent motivator for mobile health (mHealth) apps adoption [67]. mHealth apps rely on the portability and context-sensitivity of mobile computing to improve access to healthcare services that are cost-effective, scalable, and pervasive [34]. Leveraging mHealth apps would improve access to healthcare services, lower the cost and increase patients' health awareness [5]. According to the World Health Organisation (WHO), mHealth is defined as *"medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices [12]"*. There are several types of mHealth apps developed for health purposes ranging from general health apps such as decision, support, vitals, and reproductive health apps; to fitness apps for an activity tracker, nutrition tracker and mindfulness [5]. The number of mHealth apps has grown massively after launching the centralized mobile apps repositories (i.e., Google Play and Apple Store) in 2008. It has become easier for mobile developers to distribute their apps to a wide range of users [68]. Research2guidance, an organisation for providing research and consultancy for digital health, reports that 78,000 new mHealth apps were added to apps stores in 2017. The report also showed that mHealth apps downloads reached 3.7 billion and the market revenue for digital health reached USD 5.4 billion in 2017 [69].

The security of mobile apps generally and mobile health apps, in particular, becomes one of the primary concerns since mobile apps are more vulnerable to attacks [4]. Most mobile apps can collect, process, store, and transmit user and device data in and out of a device over various networks [5]. Compromising the confidentiality, integrity, and availability of such data would lead to severe consequences including but not limited to compromised devices data, and leading to financial loss [70]. In mHealth apps, security becomes a significant concern due to health-critical data privacy and integrity [5, 29]. An attack to falsify clinical measurements can lead to unnecessary care for patients as they think they are sicker than they actually are, causing medical, legal, and social concerns [16]. In addition, the lack of security awareness from end-users as they may release their health data unintentionally [4]. In fact, stolen data from other mobile domains can be contained. For example, the user may notice a suspicious transaction on his/her credit card; and hence the card can be suspended from the bank or canceled. A stolen password can be also recovered by changing it immediately. However, a stolen health data cannot be contained since health record cannot be changed, and it can be lucrative in the 'black market' [20].

Health professionals are increasingly relying upon health data which are collected via mHealth apps to make their decisions, such as dermatologic care [6], chronic management [7, 8], and clinical practices [9]. Data manipulation can significantly impact the treatment causing serious results, e.g., worsened morbidity or death [71, 72]. Whilst health regulations and laws (i.e., The US Health Insurance Portability and Accountability Act - HIPAA, European General Data Protection Regulation - EU GDPR) strive to protect medical integrity and patients' privacy by focusing on hospitals, doctors and insurance firms. Little attention has been paid to supporting mHealth apps developers by providing them with suitable guidelines for developing secure apps [3, 5].

A large part of mHealth apps' security relies on developers'[3] experience in designing and developing secure apps. According to [1, 8, 15-17], most mHealth apps have not fully implemented mechanisms to protect health data. Studies also claimed that mHealth developers might fail to appropriately implement basic security solutions such as authentication, encryption for data at rest and data in transit. It is being recognised that it is critically important to thoroughly train mHealth apps developers in implementing suitable security mechanisms to protect patients' data from being stolen or compromised [1, 16]. Hence, it is crucial to identify and synthesize the reported challenges of developing secure mHealth apps as a body of knowledge for research and practice. We have reviewed the relevant literature to determine the security challenges by focusing on the developers rather than the solutions that can be applied. The RQ for this part of the literature review is:

RQ1: *What are the challenges that developers of mHealth apps face with respect to implementing security?*

3.1.2 Research Gap

3.1.2.1 Previous Work

The challenges of developing secure software have been receiving increasing attention in recent years. A review by Kanniah et al. [73], which included 44 studies, has identified the factors that influence secure software development practices. The study finds that security skills, expertise, tools and development time are among the factors that impact secure software development. The identified factors were classified into institutional context, people and action, project content, and software development process factors. Thomas et al. [74] address the issues that security auditors face during the application review for security bugs. The study recommends further support for the development process by providing security-related tools and effective communication tools for developers'

[3] The term developer has been used in this paper referring to professionals who are engaged with engineering and development of mHealth apps.

interaction. Further support for software developers has also been recommended by providing motivation (e.g., reward or recognition) and providing solutions for technical challenges such as using third-party libraries issues. The authors recommended recruiting security experts within teams and make them available for answering questions. Raghavan et al. [75] present a model for achieving security during the Software Development Lifecycle (SDLC). Their model suggests the following factors: security policy, management support, security-related training for developers and development process control. Weir et al. [76] studied the positive factors that enhance the development of secure software. The work identified the interventions that lead to achieving security by performing a threat model, organising motivational workshops to engage team members, a continuous reminder of developers. The study also highlighted other interventions that need to be considered, such as components choice of security tools, performing static analysis, developers training, and performing penetration testing and code review.

Some studies also aimed to help mobile apps developers to develop secure apps by providing guidelines for the development process [12, 77, 78]. Given the increasing realisation of the need to provide the developers of mHealth apps with appropriate knowledge/training and support for developing secure apps, there is a critical need to identify and analyse the challenges that prevent them from developing secure apps. Our findings would contribute to a body of knowledge about the challenges that mHealth apps developers' face with respect to security.

3.1.2.2 Comparison with Prior Studies

The prior reviews [79, 80] have more focused on investigating the security measures and technical solutions employed by developers. However, a few challenges were raised in [79, 80]. Katusiime et al. [79] systematically reviewed privacy and usability issues and solutions in mHealth systems. The study considered developers' lack of security knowledge, and lack of security framework as external factors that need to be considered. Another review by Marquez et al. [80] was more on the security issues of telehealth systems. The study focused on classifying security (i.e., attacks, vulnerabilities, weaknesses, and threats), and presenting security strategies (i.e., detect attacks, stop or mitigate attacks and react to attacks) of telehealth systems. Also, the study reported some security practices that need to be ensured, such as having a discussion about architectural styles (e.g., security patterns), and engaging stakeholders during the development of an app. To the best of our knowledge, there is no SLR that explicitly investigates the challenges faced by mHealth apps developers to implement the security of mHealth apps. Thus, we aim to fill the gap and provide insights into the development of secure mHealth apps.

3.1.3 Research Method

This research has been undertaken as a Systematic Literature Review (SLR). It is one of the most widely used research methods of Evidence-Based Software Engineering (EBSE). SLR provides a well-defined process for identifying, evaluating, and interpreting all available evidence relevant to particular research. We followed the guideline of Barbara Kitchenham to perform an SLR that involves three main phases: defining a review protocol, conducting the review and reporting the review [42]. In this section, we briefly describe the main components of the review protocol and its implementation. Our review protocol has six components, including research question, search strategy, data source, study selection process, inclusion and exclusion criteria, and data extraction and data synthesis. Figure 3.1 presents a flow diagram of the literature search and articles selection results.

3.1.3.1 Research Questions

Our review's objective was to identify and codify the challenges that hinder mHealth apps' developers from developing secure apps. This review's findings would enable us to identify the potential gaps that need to be further investigated based on the developers' perspectives.

3.1.3.2 Search Strategy

We used the following strategies to form our search string: (1) identifying the major terms based on the study focus and the research question, (2) identifying all the possible keywords and related synonyms based on our experience and previous work, (3) using the Boolean "AND" to join major terms and the Boolean "OR" to join alternative terms and synonyms. We ran several pilot searches to (i) have a reasonable number of records (i.e., 1867), and (ii) ensure the search string includes the studies of which we are already aware of. Hence, our search string for this review was set as follows:

("*security*" **OR** "*insecure*" **OR** "*secure*") **AND** ("*mobile health*" **OR** "*mobile healthcare*" **OR** "*mobile health-care*" **OR** "*mobile health care*" **OR** "*telehealth*" **OR** "*mhealth*")

3.1.3.3 Data Source

We used Scopus digital library as our primary search library as there are many successful examples of other researchers, e.g., [42], who limited their search to Scopus. The Scopus indexing system has the advantages of facilitating the formulated complex search string, frequently updating and keeping track of a large number of journals and conferences in software engineering studies. Furthermore, Scopus is an indexing database that provides, names, keywords, and abstracts for all published articles. Any pointed articles can be further searched and downloaded to review the whole article regardless of which database it actually exists.

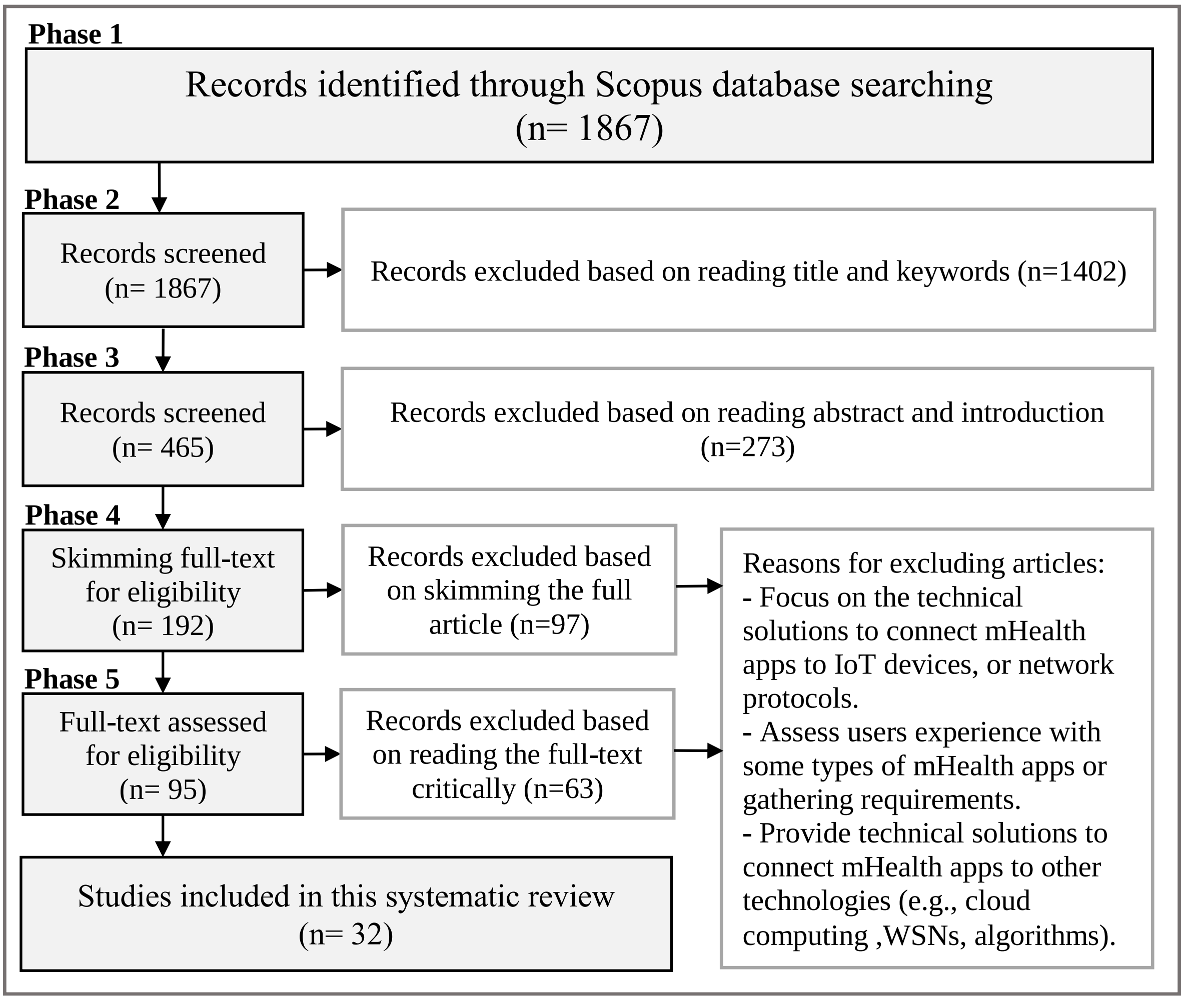

Phase 1
Records identified through Scopus database searching (n= 1867)
Phase 2
Records screened (n= 1867)
Records excluded based on reading title and keywords (n=1402)
Phase 3
Records screened (n= 465)
Records excluded based on reading abstract and introduction (n=273)
Phase 4
Skimming full-text for eligibility (n= 192)
Records excluded based on skimming the full article (n=97)
Phase 5
Full-text assessed for eligibility (n= 95)
Records excluded based on reading the full-text critically (n=63)
Studies included in this systematic review (n= 32)
Reasons for excluding articles:
- Focus on the technical solutions to connect mHealth apps to IoT devices, or network protocols.
- Assess users experience with some types of mHealth apps or gathering requirements.
- Provide technical solutions to connect mHealth apps to other technologies (e.g., cloud computing ,WSNs, algorithms).

Figure 3.1 Flow Diagram for the Selection of Articles

3.1.3.4 Study Selection Process

As illustrated in Figure 3.1, we performed several criteria for excluding studies in our SLR. Further details would be presented as follows:

Phase 1- Automatic search: We ran our search string on Scopus digital library. Thus, we retrieved a total of 1867 potential articles.

Phase 2- Title and keyword-based selection: We carefully reviewed the title and keywords to decide whether each of the retrieved articles was relevant to our SLR. We retained the papers for the next inspection when we could not decide by reading the titles and keywords. Thus, we excluded 1402 articles and included 465 articles for the next phase.

Phase 3- Abstract and introduction-based selection: We looked into the abstract and introduction for each article. This phase enabled us to include 192 articles and discard 273 articles.

Phase 4- Full paper scanning-based selection: We scanned the full article to ensure that they are relevant to our SLR objective. Thus, we included 95 articles and excluded 97 articles.

Phase 5- Critical review based selection: We critically reviewed the included papers and excluded duplication (e.g., extended versions of the studies were included, and shorter versions were excluded). Thus, we excluded 63 articles and included 32 studies, referred to as S1 to S32 (Appendix A).

3.1.3.5 Inclusion and Exclusion Criteria

For the purpose of this review, we applied predefined inclusion and exclusion criteria for papers selections. We included:

- Primary studies that focus on the development process of secure mHealth apps.
- We selected studies that were written in English published from January 2008 to October 2020 since major app stores (Google Play and Apple Store) were launched in 2008.
- We included peer-reviewed publications (i.e., journals, conferences, workshops and book chapters.

Besides excluding non-peer-reviewed studies (i.e., lecture notes, summaries, panels, and posters) and the studies which were not written in English, we excluded studies that contained irrelevant content for our review such as,

- Studies that focus on investigating technical solutions (e.g., encryption methods, authentication mechanisms, access control) for mHealth apps.
- Studies provide technical solutions to connect mHealth apps to Internet of Things (IoT) devices or cloud computing technology.
- Studies that focus on sensors layer (e.g., Wireless Sensor Network - WSNs), developing algorithms, or network protocols for mHealth apps.
- Studies that focus on mHealth apps quality or gathering functional requirements.
- Studies that examine users experience with some mHealth apps (e.g., patient management apps).

3.1.3.6 Data Extraction and Synthesis

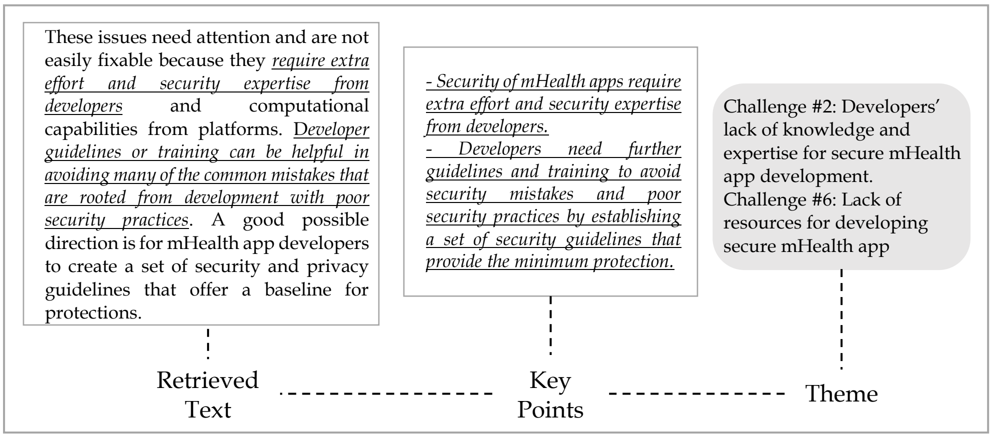
We divided the extracted data into two types, study characteristics, and challenges of developing secure mHealth apps. Our data extraction form is shown in Table 3.1 and the extracted data is available through the following link (Extracted Data). We performed descriptive statistics to analyse demographic data. We used the Endnote tool to manage the bibliography and utilised Excel spreadsheets to extract and synthesise data. We used thematic analysis, a qualitative analysis technique, to analyse and synthesize the extracted data for deriving the results for this review [47, 48]. We mainly followed the thematic analysis method's five steps as detailed below: (1) Familiarizing with data: In this step, we tried to read and examine the extracted data items. (2) Generating initial codes: In this step, we extracted the initial lists of challenges. (3) Searching for themes: We tried to combine different initial codes generated from the second step into potential themes. (4) Reviewing and refining themes: the identified challenges from step three were checked against each other to understand what themes had to be merged with others or dropped. (5) Defining and naming themes: In this step, we defined a name for each challenge. Figure 3.2 demonstrates an example, which was taken from (S4), of how our final list of challenges was identified.

Table 3.1 Data Extraction Form for our SLR

#	Data item	Description
D1	Author(s)	
D2	Year	Demographic data

D3	The Name of Publication Venue	Demographic data
D4	Title	
D5	Publication Type (i.e., journal, conference, workshop)	Demographic data
D6	Challenges that hinder developing secure mobile health apps.	RQ

To further enhance our analysis, we developed a conceptual framework to present the correlation among the identified challenges. We followed the steps of Patrick Regoniel to develop a conceptual framework that involves four steps: choose the topic, do a literature review, isolate the important variables, and generate the conceptual framework [81]. It should be noted that the initial coding was done by one person (i.e., the present author) and was reviewed and revised (followed by a discussion wherever required) with two independent researchers, Dr Leonardo Iwaya and Dr Faheem Ullah, who are experts in the field of mHealth apps, and doing SLR studies to avoid potential bias.



These issues need attention and are not easily fixable because they *require extra effort and security expertise from developers* and computational capabilities from platforms. *Developer guidelines or training can be helpful in avoiding many of the common mistakes that are rooted from development with poor security practices*. A good possible direction is for mHealth app developers to create a set of security and privacy guidelines that offer a baseline for protections.

- Security of mHealth apps require extra effort and security expertise from developers.
- Developers need further guidelines and training to avoid security mistakes and poor security practices by establishing a set of security guidelines that provide the minimum protection.

Challenge #2: Developers' lack of knowledge and expertise for secure mHealth app development.
Challenge #6: Lack of resources for developing secure mHealth app

Figure 3.2 Example of the Steps of Applying Thematic Analysis on Qualitative Data

3.1.4 Results

We now present the findings of our SLR. We classified the findings into (Section 3.1.4.1) study characteristics, (Section 3.1.4.2) challenges of developing secure mHealth apps, and (Section 3.1.4.3) conceptual framework for the identified challenges.

3.1.4.1 Study Characteristics

In this subsection, we present the demographic information based on the venues (i.e., journal, conference, or workshop) of the selected studies, as shown in Table 3.2.

Table 3.2 The Number of Selected Studies Published per Year and their Distribution over Types of Venues

Year	Journal	Conference	Workshop
2012	1	1	0
2013	0	0	0
2014	5	1	0
2015	4	2	0
2016	2	0	0
2017	3	0	1
2018	4	0	0
2019	4	1	1
2020	0	2	0

Providing such information would be useful for new researchers interested in conducting research on this particular area. We selected 32 primary studies for this review, and the complete list of the reviewed articles is available in Appendix A. All selected studies were mainly discussing the security aspects of mHealth apps. Table 3.2 shows the distribution, year of publication, and the different venues. It should be noted that our reviewed studies were published from 2012 to 2020. Out of 32 studies, we noticed that 23 studies (72%) were published as journal papers. Seven studies (22%) were published at conferences, while two studies (6%) were published as workshop papers. Furthermore, we noticed that 11 studies (34%) were published in JMIR (i.e., Journal of Medical Internet Research, and JMIR mHealth and uHealth), and two studies were published in the International Conference on Future Internet of Things and Cloud Workshops (2017, 2019).

3.1.4.2 Challenges of Developing Secure mHealth apps: Developers' Perspective (RQ1)

This subsection reports the results based on our analysis to answer the study RQ, *What are the challenges that developers of mHealth apps face with respect to implementing security?* Our analysis has identified nine challenges (referred to as **C1** to **C9**) that hinder apps' developers from developing secure mHealth apps. The identified challenges were ordered based on their frequency within the reviewed studies. The findings are detailed below. Table 3.3 illustrates the identified challenges, the key points which lead us to consider them from the reviewed studies, and the frequency of the challenge.

Table 3.3 The Identified Challenges in Developing Secure mHealth Apps

Challenge #	Key Points from Reviewed Studies	Frequency* (%)
C1. Lack of security guidelines and regulations for developing secure mHealth app	▪ Lack of security guidelines, regulations, direct laws about the security requirements, secure designing, security testing, security features that need to be employed in mHealth apps [S4, S5, S6, S7, S10, S12, S13, S15, S16, S20, S22, S23, S26, S29, S31] ▪ Lack of framework or standards (e.g., standardized policies and methodologies to ensure the security standards are met), for developing secure mHealth apps [S2, S3, S29, S31] ▪ Lack of compliance with the available guidance and/or standard [S25, S29] ▪ Challenges for the developers to deal with legal obligations, policies, and procedures [S32]	19 (59%)
C2. Developers' lack of knowledge and expertise for secure mHealth app development	▪ Insufficient knowledge of software developers about the security risks of mHealth apps [S12, S17, S18, S27] ▪ Lack of developers' security awareness (e.g., towards the potential threats of mHealth apps [S3, S9, S14, S21, S28, S32] ▪ Developers lack of knowledge towards secure coding practices, using secure APIs, and utilising up-to-date libraries [S18] or secure third-party services by mHealth apps developers that could misuse users' health data [S1, S11, S19, S24] ▪ Developers lack of knowledge about utilising security measures (e.g., (e.g., TLS security for servers, proper protection for user passwords) of mobile devices [S3, S8, S22, S25] ▪ Lack of experience in secure software development for the developers [S4] ▪ Lack of auditing security knowledge and review of what knowledge they have [S25]	18 (56%)
C3. Lack of stakeholders' involvement during mHealth app development	▪ Lack of stakeholders' participation during the development lifecycle of mHealth apps [S5, S10, S20, S29, S30] ▪ Lack of security understanding by health professionals when they engage in the development process causes poor elicitation of security requirements [S5]	6 (19%)
C4. No/little developers' attention towards the security of mHealth app	▪ Developer' assumption that users are not concerned about security [S32] ▪ Security is not the developers concern [S11, S21] ▪ Security issues should be resolved by the testers [S32]	5 (16%)

	▪ Developers with no security focus skip all security measures [S18] ▪ Developers are not considering secure design principles and privacy guidelines [S31]	
C5. Lack of financial resources for developing secure mHealth app	▪ No/low budget assigned for employing security measures [S32] ▪ Unavailability of security tools [S32] ▪ Developers lack of training in developing secure mHealth apps [S4, S5] ▪ Lack of research and development efforts to facilitate developing secure mHealth apps [S14]	4 (13%)
C6. Time constraints during mHealth app development process	▪ Rushing to the market leaves vulnerabilities in mHealth apps [S18, S26, S32] ▪ The long process of gaining consent or approving the development choices of the developers [S7]	4 (13%)
C7. Lack of security testing during mHealth app development	▪ Lack of conducting security testing [S32] ▪ Lack of conducting proper security testing (e.g., vulnerability scan) for mHealth apps [S6, S18, S23]	4 (13%)
C8. Developers' lack of motivations and ethical considerations	▪ Lack of motivations for developers during the development process of mHealth apps [S27] ▪ Developers lack of ethics during the development process of mHealth apps [S10, S30]	3 (9%)
C9. Lack of security experts' engagement during mHealth app development	▪ Lack of collaboration and discussion with security experts from the beginning of the development lifecycle of mHealth apps [S18, S32]	2 (6%)

*Frequency refers to the number of studies that indicate the identified challenge (n=32).

C1: Lack of security guidelines and regulations for developing secure mHealth app

Security guidelines refer to a set of suggested actions or recommendations for things to do or avoid during software development [82]. The security guidelines help apps developers, mostly inexperienced, adopt effective security practices and write secure codes. They contain accessible information, properly layered and searchable, with good coverage of all security aspects (e.g., cryptography, handling user input and privileges [77]). It would be ideal for clarifying that there are numerous security guidelines for ensuring the security of mobile apps (e.g., Open Web Application Security Project – OWASP). According to Nurgalieva et al. [83], the available security guidance for developing secure mHealth apps can be categorized into 1) guidelines, recommendations, or principles, 2) app development practices (i.e., applied security mechanisms) to ensure mHealth security, 3) models of user behaviour and preferences related to security and/or privacy. Such guidelines (e.g., GDPR) have had the effect of raising awareness and establishing a minimal set of expectations. However, they do not address the issue of the development of systems which meet privacy and security requirements [83]. Additionally, Assal et al. [84] indicated that security guidelines do not exist or are not mandated by the companies, or that developers might lack the ability or proper expertise to identify vulnerabilities despite having general security knowledge. Our reviewed studies, including [S3, S4, S12, S20] have pointed out a general lack of security guidelines for developing secure mHealth apps. Zubaydi et al. call for effective guidelines that can help developers build secure mHealth apps [S12]. Even though there are guidelines to protect health data (i.e., HIPAA guides), they do not provide specific instructions for developing secure mHealth apps. Furthermore, it has also been claimed that there is a lack of security frameworks, standards, compliance checklists and regulations [S22, S18, S13, S20, S2, S9]. Legal restrictions (i.e., obtaining security certification) ensure that mHealth apps development organisations are not developing vulnerable mHealth apps [S11, S12].

C2: Developers' lack of knowledge and expertise for secure mHealth app development

Security knowledge of mobile apps developers plays a significant part in developing secure mHealth apps. Lack of security knowledge would result in creating an insecure app that leaks health-critical data to attackers. The reviewed studies indicate that mHealth app developers do not have enough security education covering important security aspects. Consequently, developers follow insecure programming practices (e.g., employing improper security solutions) [S22, S19, S25], and/or improper handling of mHealth apps permissions [S23]. Furthermore, developers' lack of security knowledge leads to make wrong security choices when attaching a particular device with mHealth apps (e.g., a tracking device that helps to monitor user behaviour) [S11, S12, S18], or integrating an app with other systems [S13]. Making an incorrect security decision may allow health apps to share health-critical data with other mobile apps, untrusted apps or external hosts [S12]. In fact, mHealth apps developers were found that they make their security decisions based on their best assumptions or strategies [S24]. Thamilarasu et al. [S18] conducted a vulnerability scan that has reported 248 vulnerabilities in the top 15 Android-based mHealth apps. The study revealed that the top three most common vulnerabilities were not errors in the system, but instead, errors in the developers' choices (i.e., selecting a suitable cipher, choice of permissions to request on a mobile device). The study concluded that most vulnerabilities could have been prevented through proper coding and secure engineering practices.

Keeping in mind that threats landscapes are changing rapidly; thus, dealing with the volatile environment requires developers to keep their security knowledge sharp. Even security experts need to get their knowledge updated [85]. Despite the fact that mHealth apps vulnerabilities are frequently announced in the security-relevant knowledge banks (e.g., National Vulnerabilities Database – NVD, data breach reports) to advise developers, for some reasons (i.e., difficult to use), these security alerts are not followed or ignored. As a result, unfixed bugs might allow attackers to perform malicious activities (e.g., illegally accessing health-critical data by exploiting sensors permissions enabling them to extract data or transfer malware to an app [86]). The announcements of the identified security bugs are one way of encouraging mHealth developers to keep up-to-date with the threat landscape. Muthing et al. and Dehling et al. indicate that mHealth apps developers use out-of-date security measures [S14, S19, S23]. As a result, some mHealth apps even have previously exposed security errors [S23]. Despite the realisation of the importance of keeping mHealth developers aware of the latest security issues, there is little evidence that developers get regular formal security training to maintain their security knowledge [S24]. Lack of auditing among developers to maintain and review their security knowledge can create a knowledge gap, and lead to out-of-date security knowledge [S25].

C3: Lack of stakeholders' involvement during mHealth app development

Involving stakeholders in security requirement engineering is being recognised as a key to software success and getting effective as well as impactful outcomes [73]. Indeed, stakeholders involvement contributes to the elicitation and specification of security requirements of the developed software, yet it is difficult as developers would first spend a significant effort to understand the complexity of a problem domain [87]. In addition, more time and resources would be required. For mHealth apps, developers should refer to stakeholders (e.g., medics, patients) throughout the development process to ensure that the technology meets their needs [S10, S30]. Further, stakeholders need to be involved earlier in the development process of mHealth apps. However, development practices often include clinicians and experts but more rarely involve the target audience until evaluation [S29]. At the same time, it would be challenging for some stakeholders to have security understanding due to their capabilities when engaging them in the development process. As a result, causing poor elicitation of security requirements [S5, S20].

C4: Lack of financial resources for developing secure mHealth app

The development process of mHealth apps can be supported by using security resources to enhance secure mHealth apps development. The lack of necessary resources, such as technology, is a challenge that can directly impact the development of secure mHealth apps. For example, security tools (e.g., Zed Attack Proxy, Android Debug Bridge, Codified Security, White Hat Security, and Quick Android Review Kit)[4] are supporting resources to facilitate writing secure code, and testing apps during the

[4] https://owasp.org/www-project-zap/
https://codifiedsecurity.com/
https://developer.android.com/studio/command-line/adb

development process. They help developers catch errors that they might be unaware of and adjust their code accordingly before releasing an app. Wurster et al. [88] argued that not all software developers are security experts, and there is a need to use suitable security tools during a development project. Security tools for mobile apps have received a lot of attention from researchers. A recent security tool, called FixDroid [89] can show warning messages with recommendations to fix errors during the coding phase. It proved its effectiveness by improving the security of the written code, it is limited to Android apps developers, and it is not widely known.

Similarly, software libraries can be used as supporting resources to facilitate the software development process. Such libraries help developers reuse specific code for certain goals and support access to hardware and software that might be needed. Yet, it can be challenging for developers to know which library to trust while developing mHealth apps. There can be a risk of data leakage by using untrusted libraries [S16, S13]. Some libraries, especially the open-source ones, may collect data about users without developers being aware of, leading to data privacy breaches [90]. Furthermore, using untrusted third-party libraries to integrate the mHealth app with Electronic Health Record (EHR) can lead attackers to gain unauthorised access to patients' data [S13].

Older versions of security resources (i.e. tools and libraries) also contain known vulnerabilities [S18]. Most of the security resources are often updated to address security-related issues and introduce new functions; hence, it is important to be aware of and use the latest security tools and libraries. Therefore, developers' security knowledge of the adopted security resources can significantly impact the developed app's security. Besides being aware of the relevant security resources, it can be difficult for developers to learn to use them within the time and resources available for a project [S25, S17].

C5: No/little developers' attention towards the security of mHealth app

Incorporating security should be considered ideally throughout the SDLC from requirement analysis to the deployment phase [91]. In fact, addressing security at later stages of app development or after releasing the app in the form of security patches can be a costly exercise and can introduce new vulnerabilities [92]. Studies, such as [S11, S21, S31], found that mHealth apps developers pay little or no attention to the security of mHealth app. This issue can be seen for a few reasons including (1) developers' assumption that users are not concerned about security, (2) developers' assumption that security should be handled by app testers, and (3) developers with no security focus would even skip all security measures to resolve other quality attributes including usability and performance [S18, S32]. Therefore, it is important to come up with effective mechanisms for overcoming developers' lack of attention to security.

C6: Time constraints during mHealth app development process

Due to business pressures (e.g., rushing to the market), delivering an app on time tends to be the main aim mHealth apps developers to try to satisfy customers and avoid extra costs. High workload and tight timeframes require mHealth apps developers to put more effort to meet functional requirements as a primary task [S18, S26, S32]. It also affects their attitude and behaviour towards addressing security (e.g., underestimating risks, assuming attackers will not realise the weaknesses) and dealing with security after releasing an app [91]. This approach leads to insecure mHealth apps and increases the cost and introduces new vulnerabilities after fixing the existing vulnerabilities [93]. It is estimated that the cost can be 30 to 100 times more expensive to retrofit security compared with incorporating security from the beginning [94]. Besides, the speed of delivering apps will also affect team members to share and convey security knowledge among mHealth apps developers [95]. Furthermore, the long process of gaining consent or approving the developers' choices by their managers can be an issue [S7]. As a result, making the process of having their opinion on a certain task take longer. Hence, this lead to skipping security issues that need to be fixed.

C7: Lack of security testing during mHealth app development

Security testing is one of the essential phases of the mHealth apps development lifecycle. Security testing helps determine the quality of apps by ensuring all the security requirements are met. Security

https://securityonline.info/quick-android-review-kit/
https://www.whitehatsec.com/

testing for mHealth apps, in particular, will help to see how an app will react against different attacks (e.g., unauthorised access to health data, tampering health data or reporting invalid health data to health professionals [S11]. Security testing of mHealth apps can be overlooked since it can be a challenging task for developers. Several factors can affect performing security testing including the absence of security testing tools, lack of effective and well-known testing guidelines, cost of performing app testing by a third-party organisation, or lack of security expert with a software development organisation [S23, S18, S6]. Consequently, this would release mHealth apps without conducting security testing, leaving an app at high risk [96]. Wurster et al. indicate that security testing is not a first-choice task for developers, and their main job is completing the required features [88].

C8: Lack of security experts' engagement during mHealth app development

A security expert, security leader or security champion within an organisation plays a vital role during the mHealth apps development process [S7]. Besides their development activities, they direct mHealth apps' developers on secure development practices and perform a security review to ensure their code does not have security defects. A security expert can encourage developers to achieve security goals and educate other developers about potential threats and solutions [S14]. The lack of security experts within a software development team can lead to failures in applying proper security controls by mHealth apps developers. Besides, the lack of availability of security experts would be a challenge for developers [S7]. As a result, lack of constructive feedback that prevents developers from (1) acquiring security knowledge, (2) gaining hands-on experience, and (3) developing apps that are secure by design.

C9: Developers' lack of motivations and ethical considerations

Motivation refers to the driving force behind all the actions of developers during development. It has been recognised as a critical success factor for software projects. Motivation can be seen differently based on developers and an organisation's size [97]. The research on security practice indicates that many security incidents are mainly caused by humans, rather than technical failure [98]. Developers with low motivation were found to be one of the most frequently cited causes of software development project failure [99]. Xie et al. [100] present the reasons that make software developers make security errors. The study concluded that most software developers have a "not my problem" attitude, which indicates that software developers are the source of security errors due to their attitudes and behaviours. In mHealth apps development, in particular, studies such as [S10, S27, S30] reported that developers' lack of motivations and ethical consideration is a challenge that hinder developing secure mHealth apps.

3.1.4.3 Conceptual Framework

Based on our analysis of the extracted data, we propose a conceptual framework, as in Figure 3.3, that represent the challenges of developing secure mHealth apps. Jabareen in [101] defined conceptual framework as "*a network, or a plane of interlinked concepts that together provide a comprehensive understanding of a phenomenon or phenomena.*" Figure 3.3 presents a conceptual framework for correlating the identified challenges.

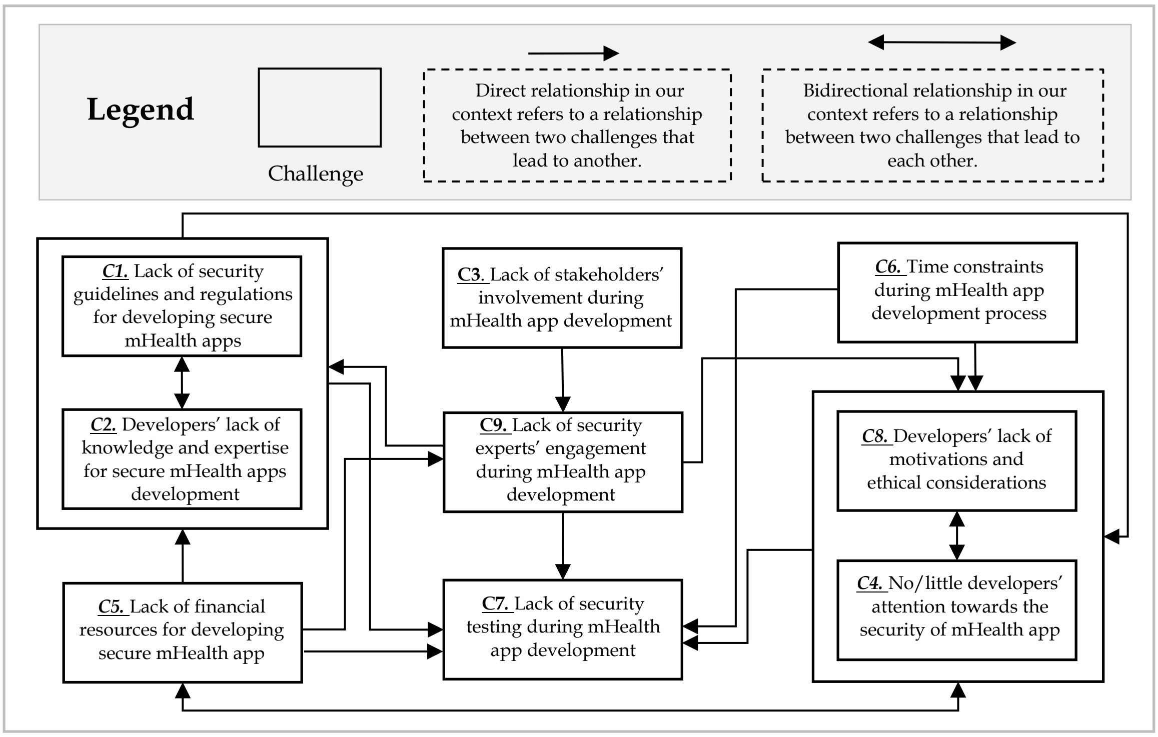

Legend
Challenge
Direct relationship in our context refers to a relationship between two challenges that lead to another.
Bidirectional relationship in our context refers to a relationship between two challenges that lead to each other.
C1. Lack of security guidelines and regulations for developing secure mHealth apps
C2. Developers' lack of knowledge and expertise for secure mHealth apps development
C3. Lack of stakeholders' involvement during mHealth app development
C9. Lack of security experts' engagement during mHealth app development
C6. Time constraints during mHealth app development process
C8. Developers' lack of motivations and ethical considerations
C4. No/little developers' attention towards the security of mHealth app
C5. Lack of financial resources for developing secure mHealth app
C7. Lack of security testing during mHealth app development

Figure 3.3 A Conceptual Framework for Correlating the Challenges in Developing Secure mHealth Apps

Based on the results of Table 3.3, we identify the most critical challenges for developing secure mHealth apps. Critical challenges for developing secure mHealth apps can be determined if a specific challenge has a frequency of ≥50% of the selected studies. This criterion has been used by other researchers in different domains [102-104]. As in Table 3.3, the percentages of frequency are shown for each challenge in the reviewed studies. By using this criterion, we conclude that there are two main critical challenges which are: lack of security guidelines for developing secure mHealth apps (19 out of 32 studies, 59%), and developers' lack of security knowledge and expertise for secure mHealth apps development (18 out of 32 studies, 56%).

Despite the fact that other challenges were given less attention by the reviewed studies (i.e., 19% for C3, 16% for C4, 13% for C5-7, 9% for C8, and 6% for C9); some challenges have a direct relationship with other challenges as we indicated earlier (e.g., poor security decisions during mHealth apps development is related to insufficient security knowledge of developers). Consequently, there will be an impact on the development process of mHealth apps. Therefore, we believe identifying these challenges would help mHealth apps development organisations to evaluate their security practices and readiness in implementing security in mHealth apps projects.

3.1.5 Discussion

3.1.5.1 Principal Findings

Whilst mHealth apps enable healthcare services, the security of end-users health data remains a challenge. This review is aimed to identify the challenges that prevent developing secure mHealth apps based on the existing literature. We identified nine challenges based on the analysis of the data extracted from 32 articles. The identified challenges include: 1) lack of security guidelines and regulations for developing secure mHealth apps, 2) developers' lack of knowledge and expertise for secure mHealth app development, 3) lack of stakeholders' involvement during mHealth app development, 4) no/little developers' attention towards the security of mHealth app, 5) lack of resources for developing secure mHealth app, 6) project constraints during mHealth app development process, 7) lack of security testing during mHealth app development, 8) developers' lack of motivations and ethical considerations, and 9) lack of security experts' engagement during mHealth app development. We noticed from the literature that there is an emphasis on presenting the security issues of mHealth apps and how they can be resolved (e.g., presenting a security framework, providing secure mHealth app development recommendations, evaluating the security of existing mHealth apps, etc.). However, little attention has been given to the human factor during the development process of mHealth apps (i.e., non-technical solutions). Hence, it would be critical to recognise the security challenges that mHealth apps' developers face during the development process.

Sufficient security knowledge for mHealth apps' developers is one of the key factors that would help to develop secure apps. Security knowledge can be discussed as the type of required security knowledge and the sources of acquiring that knowledge. According to Barnum et al. [82], there are seven security knowledge categories for developing secure software including knowledge of principles, guidelines, rules, attack patterns, vulnerabilities, exploit and historical risk. While the presented set of security knowledge provides a perfect foundation for enhancing security, yet it would be a bit challenging for developers since security knowledge is scattered all around. By considering security knowledge of vulnerabilities as an example, attackers can find a single vulnerability to exploit the app (i.e., launching an attack). In contrast, developers should be aware of all security vulnerabilities and apply proper security measures and patches, which can be a daunting task. mHealth apps, more specifically, are connected to IoT devices which make securing the apps a challenge. Sikder et al. [86] indicated that attackers could illegally access health data through exploiting sensors permissions', which could enable them to extract data and transfer malware to the app. Therefore, further support for mHealth apps' developers' security knowledge is needed to cope with the rapid changes in security knowledge.

Likewise, using trustable sources (i.e., tools and libraries) would be challenging for developers to have an awareness of their secure usage. So, we suggest further improvement that needs to be done to facilitate the job of mHealth apps' developers by exploring the list of trustable sources. Identifying the trustable sources with their policies, terms and conditions of usage and the proper ways of getting their updates would help mHealth apps' developers to develop secure apps. At the same time, following this approach would help to disseminate and provide security knowledge for mHealth apps developers through trusted sources.

3.1.5.2 The Role of Security Experts within mHealth Apps Development

"A critical challenge facing software security today is the dearth of experienced practitioners"— Barnum and McGraw [82]. A report by IBM showed that there is a dearth of security experts in mobile apps development. Only 41% of the participants indicated that their organisations had sufficient security expertise [94]. Hence, having a security expert can be a strategic advantage for an organisation. The role of security experts is quite crucial in developing secure mHealth apps. We conclude from Figure 3.3 that the lack of security experts is already linked with most of the challenges. Without security experts in a team, the required security knowledge will be missing (i.e., what security guidelines need to be followed, what security tools are available to be utilised and which libraries can be trusted). As a result, developers' security knowledge would remain insufficient. Besides, the lack of security experts within mHealth apps development organisations can lead to poor coding practices, rushing to deliver an app without even performing security testing. Furthermore, collaboration and social interactions with security experts and other team members would have a significant impact on security. As a result, removing the boundaries and stimulating the formation of common interests, in turn, support exchanging knowledge and ideas [97]. Also, it is a good practice to exchange security knowledge, leverage that knowledge within the project, and acquire new knowledge.

3.1.5.3 Importance of Security Knowledge and Expertise for Secure mHealth Apps Development

Our analysis showed that developers' lack of security knowledge and expertise for secure mHealth apps development is correlated with most of the identified challenges. For instance, developing secure mHealth apps requires decent knowledge about security guidelines, security tools, and trusted libraries (i.e., awareness of how, when and why they should utilise them). It is worth mentioning that the development of secure mHealth apps has become complex and challenging. mHealth apps require connecting with external sensors or devices, e.g., wearable devices, implantable devices [86]. Nevertheless, providing the required learning resources can be underestimated by mHealth apps development organisations [105]. Thus, organisations are required to provide security material to allow developers to learn to connect mHealth apps with emerging technologies, i.e., the Internet of Things (IoT). Providing resources to support secure mHealth app development would contribute to filling the security knowledge gap and help to open developers' mindsets to security errors that need to be avoided [85].

We have presented the findings from an SLR in the previous section based on our research question. In this section, we discuss our findings and highlight some potential future directions.

3.1.6 Future Work

The results of our review enabled us to propose the following areas that warrant future research on the secure development of mHealth apps

3.1.6.1 Challenges and Solutions to Develop Secure mHealth Apps with Real-World Practitioners

In this review, we have identified the challenges that hinder developing secure mHealth apps based on SLR. Our literature review revealed a need for an empirical study to investigate the challenges of real-world practitioners to validate our results. Such research would enable us to compare the identified challenges identified in the literature with real-world practices for better understanding. Furthermore, it also revealed the importance of investigating the practices and solutions that real-world practitioners use to overcome the identified challenges. As a consequence, this would allow us to define which challenges are correlated with which practices. Hence, identifying the challenges and solutions would help us extend the current conceptual framework and provide a body of knowledge for secure mHealth apps development.

3.1.6.2 Developers' Motivations and Ethical Considerations for Developing Secure mHealth Apps

Since motivations and ethical considerations play an essential role in secure mHealth apps development process, we assert that there is a need to conduct an empirical study to understand the developers' motivational factors, and what inspires them to ensure the security of mHealth apps (e.g., security leaders, with the team, reward, recognition, career path or promotion). Such a study can be further investigated by collecting quantitative data (e.g., hypothesis testing) and/or qualitative data. This would create a better understanding and help mHealth apps development organisations to realise and focus on motivational factors.

3.1.7 Limitation

One of the potential threats to our SLR can be missing or excluding relevant studies. To mitigate this threat, we used Scopus library as our data source. Scopus is considered the largest indexing system that provides the most comprehensive search engine among other digital libraries [106]. Scopus enabled us to get a reasonable number of studies (1867 articles). Furthermore, we tested our search string based on the pilot search to improve it and reach the relevant studies for this review. We selected the study based on predefined inclusion and exclusion criteria. However, including and excluding studies can be impacted by researchers' subjective judgement. To mitigate this threat, the reasons for excluding the papers were recorded and reviewed by two independent researchers (who have been previously mentioned). Their inputs helped to improve paper selection through conducting a random cross-check. Any disagreements were resolved through a discussion.

Our research can be influenced by the researcher's bias in extracting data from the reviewed studies, which may negatively affect the findings. To overcome this threat, we extracted data based on a predefined data extraction form, as in Table 3.1. To mitigate the researcher's bias in data extraction and synthesis, three independent researchers randomly verified the key points and themes derived by the first author through discussions.

3.2 Security of mHealth Apps: End-Users' Perspectives

3.2.1 Introduction

Smartphones become an essential part of our daily life as their functionalities have highly improved. Their capabilities are no longer limited to calling and texting, it even goes beyond that due to their advanced computing features, and enhanced preferences that can perform different tasks easily (e.g., sending e-mails, tracking through Global Positioning System (GPS), taking images, etc.). Accordingly, smartphones become a promising technology to be used for many aspects to enhance the quality of life.

Ideally, their embedded sensors, as well as the software applications (apps) make smartphones feasible to be used by many business apps and support even healthcare practices. Mobile Health (mHealth) apps can be utilised to manage patient health and share data with the assigned health professionals to allow further judgment anytime and from anywhere [107]. Leveraging mHealth apps will not only improve access to healthcare services. But also lower the cost and increase health awareness for patients. There are several types of mHealth apps that have been developed for health purposes ranging from general health apps such as decision, support, vitals, and reproductive health apps; to fitness apps for an activity tracker, nutrition tracker and mindfulness [5].

The growth of the mHealth apps market is rapidly increasing due to the adoption of smartphones by individuals as well as the continued heavy investment into the digital health market (e.g., health providers and governments) [108]. A report by Zion market research showed that mHealth apps market was valued at approximately USD 8.0 billion in 2018 and is expected to reach up to USD 111.1 billion by 2025 [109]. One of the advantages of using mHealth apps is to help patients who are suffering from chronic diseases to monitor their health conditions. World Health Organisation (WHO) reported that chronic diseases are the main cause of death more than any other diseases. For instance, cardiovascular disease in the US affects around 84 million people, and about 610,000 deaths occur each year [110]. The use of mHealth apps is not only limited to monitoring current patients, but also combating the risk factors and applying early detection through monitoring end-users health to report abnormalities as soon as they are discovered. As a result, applying early treatment before reaching the epidemic proportions stage [111].

Nevertheless, the security of mHealth apps is very critical by the nature of health data as well as the laws which need to be maintained. Security incidents have increased lately targeting the health care sector. Several statistics highlighted recent health data breaches. For example, a report by Verizon 2018 data breach revealed that the healthcare industry has the highest number of data breaches and 79% of the compromised data in the health domain was medical data [112]. For a large-scale IT organisation, that increase can represent hundreds of millions of dollars as costs for identity-theft protection, IT forensics and government fines [20]. The employed security features in mHealth apps may not be sufficient to guarantee security, there is a need to complement human-centric knowledge and practices to protect health data. Thus, a clear understanding of end-users security issues and concerns about using mHealth apps is needed. Consequently, this would provide us with the required knowledge-base that help to conduct further studies. Thus, we reviewed the literature to find the answer for ***RQ5:*** *What are the security knowledge and perceptions of end-users about using mHealth apps, which have been reported in the literature?*

3.2.2 Results of Reviewing Literature

The related work on this topic can be generally classified into two categories, i.e., (i) end-users' security awareness about mHealth apps (Section 3.2.2.1) and (ii) end-users' awareness of privacy policies for mHealth apps (Section 3.2.2.2). Table 3.4 helps to objectively compare our research in terms of its scope and contributions in the context of existing work.

3.2.2.1 End-users' Security Awareness of mHealth Apps

In contrast to the general purpose of mobile apps, mHealth apps collect, process, and exchange a multitude of private data that can be vulnerable to various security threats such as tempering of medical records, data sniffing for targeted advertisements, and identity theft [1]. For example, the magnitude and variety of private data including personal details (e.g., age, gender, location coordinates etc.) and health-critical information (e.g., disease symptoms, clinical reports, medical prescriptions etc.) make it challenging for end-users to protect sensitive information from undesired access [16, 71]. From the perspective of mHealth app providers, in addition to ensuring that secure mHealth apps have been delivered by developers, end-user training and security awareness must be treated as a priority before deploying and operationalizing mobile health systems [4]. On the contrary, some recent studies highlighted that a lack of knowledge or understanding of end-users regarding security features is still being overlooked as a threat [4, 18, 113, 114]. In the context of mHealth SDCL, the prime importance is given to the development of security-aware apps with developers and mHealth providers having a collective assumption that the delivered app is secure. Despite the fact that app(s) delivered by following a secure SDLC can have well-implemented security features, for end-users, such complex implementations could be either hard to understand, utilise, or require human intervention to operate [38]. As a typical example, to avail of nearby healthcare services or consult available medics, end-users may end up providing excessive permissions such as current location, activity, or active social contacts without being notified [4]. Understanding the security preferences of end-users can help app developers and providers to maintain the required balance between security and usability of mHealth apps [23].

Security perceptions of end-users: End-users' security perceptions of using mHealth apps can vary based on the type and context of data that is handled by the apps. Specifically, a study by Atienza et al. [24] reported that end-users' perceptions and attitudes towards the security of mHealth apps are highly contextualized based on the type of data collected by an app, time and context of access, i.e., *who* accessed the data, at *what* time they accessed it and *why.* Alternatively, some end-users do not mind sharing their health-specific data on social networks, gathered by health and fitness monitoring apps (e.g., workout, walking distance, and burnt calories). An empirical study used mixed methods to collected qualitative data using six focus groups of 44 end-users and interviews with five individuals [53]. Most of the study's participants affirmed that one of the barriers to continue using mHealth apps is sharing personal information, that might be exploited by a third party (e.g., insurance companies or advertisers). Such data sharing, despite having social implications, is perceived as volunteering efforts to encourage others to engage in healthy routines and lifestyles or obtain support and feedback from social contacts. In a study by Zhou et al. published in 2019 [23], the authors sought to identify the desired security features that enhance the trust of end-users. The study was conducted through semi-structured interviews with 117 participants. The participants agreed that their confidence level increases when using mHealth apps that enable end-users to adjust security settings, enforce regular updates for passwords, and allow monitoring data access via access logs. Moreover, the participants suggested biometric verification, providing end-to-end-encryption for data-in-transit and data-at-rest, and allowing end-users to wipe up the device remotely, once it is lost or stolen. However, the results cannot be generalized as the study covered only young and healthy participants. Another study by Zhou et al published in 2018 [115] investigated whether a brief security education offered in a mHealth app (i.e., Security Simulator app) can change end-users' security behaviour in terms of choosing appropriate security settings. The participants were asked to make security selections in the developed app before and after they viewed the consequences of security features. The participants' selections before and after the security education were compared to determine the effectiveness of security education to improve security awareness. The findings of the study concluded that simulation-based education is helpful in changing end-users' security behaviour and helps them to select stronger security measures.

End-users' security knowledge and preferences for mHealth apps: The low knowledge of security and privacy could hinder the adoption of mHealth apps by end-users. At the same time. it would be challenging to know what security preferences mHealth apps users are looking to have since most of them have little or no IT background. Generally, mHealth apps can be secured by addressing the security mechanisms (e.g., encryption, authentication, secure storage, access control) to achieve confidentiality, integrity, and availability [31]. Although mHealth apps are getting more attention from both health providers and users, yet, studies reported that low knowledge of security features for the user is the main concern [4, 18, 113, 114]. A study by Mylonas et al. in 2013 [22] indicated that today's smartphones are already supported with security features (e.g., device lock mechanisms, remote data wipe). By using the device capabilities, users can have strong protection for their health data; nevertheless, a recent survey involved more than 450 smartphone owners clearly indicated that they do not use these security features [23].

Due to the low knowledge, users might give more permission for the app to share their health data or allow other apps to access their health data without realisation [4]. As a result, low knowledge on how to manage apps permission of the device could lead to allowing third-party organisations to access users' health data. In addition, the low knowledge of authentication methods can lead to insecure apps (e.g., creating weak passwords and easy to guess, using the same password for all the accounts). Health professionals (i.e., doctors) have also low knowledge of security features. They can create some security problems when they use their own device because of their Information Technology (IT) literacy. A recent study published in 2020 by Wani et al. [116] reported that health professionals use their own devices to store patients' data. Mostly their devices have no authentication method or lock mechanism which make patients' data vulnerable in case the device is lost or stolen. Further, health professionals usually get more access privileges than they actually need. The problem relies that they are running other mobile apps on their devices which request more access permissions to mHealth apps.

Use of personal devices for mHealth systems: In clinical setting environments, health practitioners are often encouraged to use their own devices (i.e., Bring Your Own Device - BYOD) [114]. Personal devices can be customized and convenient for practitioners to work with mHealth systems; however, such devices lack strict authentication or lock mechanisms, which make end-users' data vulnerable to undesired access. Considering the BYOD scenario, healthcare professionals usually get more access privileges as administrative users of mHealth apps. Therefore, when such professionals run other mobile apps, that frequently access device data, in parallel to mHealth apps, it can compromise the security and privacy of health-critical data. Modern devices with up to date security patches are equipped with security features including device lock mechanisms, end-to-end encryption and remote data wiping for enhanced protection [22]. Wani et al. [116] indicated that there is a lack of policy and guidelines for health professionals and that can leave patients' health data are vulnerable. In a recent survey study by Zhou et al. published in 2019, more than 450 smartphone owners clearly indicated that they did not use the security features offered by the devices such as frequent password updates, biometric verification or mechanisms for controlled data access [23].

3.2.2.2 End-users' Awareness of Privacy Policies for mHealth Apps

Privacy policies represent a set of legal statements put forward by regulatory bodies. These regulatory statements must be incorporated in mHealth systems to make data collection, processing, and transmission transparent to data contributors, e.g., end-user [117]. As a standard practice, privacy policies are presented to end-users before the installation of mHealth apps. A lack of awareness of end-users about privacy policies can be mainly due to (i) mHealth apps providers lacking clarity and transparency in presenting such policies or (ii) end-users themselves that overlook or ignore reading through such policies to understand their consequences [113, 114]. A study by Parker et al. in 2019 [114] conducted content analysis to investigate privacy issues for 61 mental health apps. The results of the study suggested that in most cases, privacy policies are ambiguous and there is a need to provide information to end-users about how and when their health data would be collected, retained, or shared with any third parties. The study found that most of the analysed apps encourage end-users to share their health-critical on social networking platforms without rationalizing the social and legal consequences [114]. Moreover, in many cases, privacy policies are hard to read and understand due to the use of complex language and notations.

A study by Nicholas et al. in 2017 [118] performed a content analysis of consumer perspectives on mHealth apps for bipolar disorder patients in particular. The study's participants showed that they have no problem upgrading apps or buying some features that can help to maintain their privacy. There is a need to increase the privacy awareness of end-users and to achieve that mHealth providers should support the explicit presentation of privacy policies as part of user training [113, 114]. We assert that privacy policies should answer some fundamental questions about end-users' rights regarding their private information, such as how to terminate data collection, how to remove health data from an App's servers, and how and to whom end-users can complain [18, 23, 114, 119]. In the absence of explicit presentation and users' training regarding privacy policies, even the advanced security features cannot guarantee the integrity of personal information and health-critical data [115].

Conclusive Summary: We now provide a conclusive summary and comparative analysis of the most relevant existing research with positioning our research study in Table 3.4. To compare, we classify the most relevant research among three categories namely (a) security-aware usage [23, 24, 40], (b) security policies for secure usage [53, 115], and (c) security-aware development of mHealth apps [34], as in Table 3.4. Comparative analysis is based on four criteria in Table 3.4: (i) *research challenge(s)*, (ii) *focus and contributions*, (iii) *evaluation context*, and (iv) *research limitations*. The *study reference* points to an individual research work under discussion and its *year of publication*. For example, a study [34] published in 2020 aims to address the challenges pertaining to developers view on secure SDLC for mHealth apps. The study focuses on challenges, practices, and motivators for secure development of mHealth apps. The research has been evaluated based on a survey of 97 mHealth app developers; however, the number of participants and singular source of data (i.e., web-based survey of respondents) represents study limitations [34].

Based on the data in Table 3.4, to the best of our knowledge, there has been no empirical study to investigate the end-users' perspectives and their security awareness about using clinical mHealth apps. The scope of our proposed study is precise in terms of investigating clinical mHealth apps such as patient management systems that handle highly sensitive health-critical data and personal information. Our study is expected to provide an in-depth view of the security awareness of end-users and determine end-users' security knowledge, attitude and behaviour about using mHealth apps, as in ***RQ6***. Our study also aims to identify how end-users are influenced by their knowledge, attitude, behaviour when they use mHealth apps, as in ***RQ7***. Further, we aim to identify specific security features that may enhance end-users confidence in using mHealth apps, as in ***RQ9***. We also aim to determine the various security-related challenges faced by end-users and their impact on data privacy and app's usability, as in ***RQ10***. Moreover, we present the implemented methods to ensure end-users have the underlying knowledge for mHealth app they use, as in ***RQ11***.

Table 3.4 Comparative Analysis of most Relevant Existing Studies Compared to the Study Presented in Chapter 5, and Chapter 6

Study Reference	Research Challenges	Focus and Contributions	Evaluation Context	Research Limitations	Pub. Year
Empirical Studies on Security-aware Usage of mHealth Apps					
[24]	Investigated the security and privacy of mHealth apps from end-users' views.	- Users' attitude toward security - Users' concerns about security	- Focus Groups (256 participants)	- Limited to the functionality of apps - Source of data collection	2015
[23]	Investigated security barriers for end-users of mHealth apps.	- End-users' security and privacy - Desired security features	- User Survey (117 participants) - Focused Group Interviews	- Diversity of participants - Bias in data collection	2019
Investigating Impacts of Security Policies on Usage of mHealth Apps					
[115]	Methods to encourage end-users of mHealth apps to follow stronger security measures.	- Impacts of security settings - Simulating security scenarios	- User Survey (66 participants) - User Interviews	- Limited to a specific group of end-users, i.e., young and highly educated (Bachelor's degree or higher).	2018
[53]	Empirical analysis of end-user's perceptions towards using mHealth apps.	- Usability patterns of app - Users' security knowledge	- Focus Groups (44 participants) - Individual Interviews (5 participants)	- Lack of app usage experience - Number of Participants	2016
Survey of Security-aware Development of mHealth Apps					
[34]	Investigated developers' perspectives on secure SDLC for mHealth Apps.	- Security challenges for SDLC - Security practices for SDLC - Motivating factors for SDLC	- Developers' Survey (97 participants) - Qualitative Analysis	- Number of participants - Source of data collection (Survey only)	2020
Proposed Study in Chapter 5 and Chapter 6	Empirically investigate security awareness of end-users of mHealth apps (clinical settings)	-Security knowledge, attitude and behaviour. - Security perception (existing vs. desired features) - Security challenges (security vs. usability) - Security knowledge (self vs. training)	- End-users' Survey (101 participants) - Qualitative Analysis - User perception taxonomy	- Diversity of participants - Source of data collection	N/A (conducted in 2020)

3.3 End-Users' Security Behaviours towards Using mHealth Apps

3.3.1 Introduction

Nowadays, smartphones have become an indispensable part of both our personal and working lives. The ownership of smartphones has increased sharply in the past few years. According to Statista, the proportion of people who own smartphones reached 78.05% of the global population in 2020 [120]. Using the different mobile applications (apps) made performing tasks easier. Installing apps from the major app repositories, such as Android and iOS, has become a straightforward process that can be done by almost every mobile owner. Nevertheless, mobile devices connectivity to cyber space has made them more prone to numerous security threats [55]. It has been reported that mobile devices are three times more vulnerable to phishing attacks than personal computers [121]. In fact, some installed apps can unintentionally be granted access by the users to all of a device's resources, allowing the app to use and share end-users' data. As a result, data, including health-critical data, can be leaked to an external host or a third party through excessive app permissions [4]. A recent research study, published in 2020 by Molyneaux et al. [121], found that it is difficult for end-users to make security-related decisions when facing security threats. Indeed, most end-users are unaware of such threats to their data, or are unable to understand the technical mechanisms behind data leakage, which leads them to ignore the associated security risks [121].

Measuring the security awareness of end-users is a vital step toward helping stakeholders to develop apps that interact with end-users to protect their health data. The main objective of this literature review is to gain an understanding of existing methods to measure the security awareness of end-users of mobile apps. It also investigates the security characteristics in the context of mHealth apps that need to be measured. Such an investigation enables an understanding of the effectiveness of the various mechanisms and how it is possible to conduct further research studies. Therefore, the literature review seeks to answer ***RQ11****: What are the security characteristics in the context of mHealth apps that need to be measured? And how they can be measured?*

3.3.2 Results: Measuring Mobile Apps End-users' Security Awareness (RQ11)

Reviewing the literature enabled the building of a solid base for designing the research study protocol (i.e., Section 2.4.1). The focus of this literature review is to understand how to measure the security awareness of end-users of mobile apps and what security characteristics can be measured, as in ***RQ11***. The previous literature review (Section 3.2), and our recent studies [40, 52] provided us with an overview of the security issues, concerns, and preferences of mHealth apps from end-users' perspectives. Therefore, it was possible to answer the second part of ***RQ11*** (i.e., security characteristics in the context of mHealth apps that need to be measured). This review attempts to understand existing methods to measure the security awareness of mobile end-users, and their limitations to establish a solid foundation for designing the research study protocol (i.e., Section 2.4.1). This section presents an overview of existing studies that measured the security awareness of the end-users' of mobile apps. This section presents a conclusive summary and comparative analysis of the most relevant existing research, as in Table 3.5.

Previous studies have used two common methods to measure the security awareness of end-users of mobile apps, namely, survey-based studies, and action-based research. Each method is detailed with some examples.

3.3.2.1 Survey-based Studies

The most common approach for assessing the security awareness is through questionnaires (i.e., surveys, interviews, focus groups, etc.). In this approach, researchers request the participants to answer self-reported questions about what security-related actions they have taken in the past, or intend to take in the future [122]. Hereafter, a few studies that fall into this category will be provided. A recent study, published in 2020 by Aljedaani et al. [40], explored the security awareness of end-users of mHealth apps by utilising the HAIS-Q model. The study aimed to measure the security knowledge, attitudes, and behaviours of end-users regarding the use of clinical mHealth apps. Four security issues were investigated (i.e., privacy, access control, encryption, and authentication). The study is based on a survey of 101 end-users who use mHealth apps in clinical settings. The study revealed that despite having the required knowledge, end-users did not demonstrate appropriate behaviour when dealing with the existing security measures. Yet, the study findings mainly relied on participants' self-reported behaviour, and with such a data collection method, there is potential for bias. A study by Alotaibi et al. published in 2016 [123] investigated the cyber security awareness of computer and mobile users by focusing on three contexts, namely, cyber security practices, cybercrime awareness, and incident reporting. A questionnaire-based survey was used to collect data from 629 participants related to cyber security awareness in Saudi Arabia. The statistical analysis (i.e., Chi-square, correlation of survey items, Cronbach's alpha) for the obtained data found that although the participants had a good knowledge of IT, their awareness of the threats associated with cybercrime, cyber security practices, and the role of government and organisations in ensuring information safety across the Internet, is very limited.

A study by Zeybek et al. published in 2019 [124] investigated the security awareness around the use of mobile devices. The study mainly focused on security habits (i.e., installing and/or rejecting an app's permissions, using an antivirus app, locking the screen, frequently updating apps, and installing apps from an official store). A questionnaire was used to collect data from 120 employees in a public institution. Due to the fact that the study participants were aware that senior managers might be reviewing the outcomes, they may have reported their best habits; thus', the data could be biased. The study concluded that awareness training and malware analysis through internal experts or external institutions are required. A study published in 2017 by Watson et al. [125] investigated the security awareness of mobile devices users through surveying 94 participants. The study instrument (i.e., questionnaire) was developed based on the literature and a list of mobile security recommendations was compiled (i.e., device settings, user behaviours). The study found that participants, especially those without strong IT knowledge, tend to ignore or are unaware of many critical security options.

A study by Mylonas et al. in 2013 [22] investigated the security awareness of smartphone users through a survey of 458 participants. The study focused on enabling security controls on users' devices, finding out whether the users consider security when choosing or downloading apps, and whether they trust an app's repository. One of the study findings was that smartphone users were not adequately prepared to make appropriate security decisions. Further, users were poor at adopting 'pre-installed' security controls, such as encryption, remote data wipe, and a remote device locator. However, the study had some limitations that could have affected their results, such as focusing on self-reported behaviour without conducting further evaluation, and potential bias in their sample (the majority were males aged 15-30). A study by Gkioulos et al. published in 2017 [126] investigated the security awareness of end-users when using mobile devices, and included tablets and laptops users. The study was conducted through a survey performed across a multinational sample of digital natives (born 1987-1997). It investigated security awareness in five focus areas: (i) use of mobile devices; (ii) connectivity and network access; (iii) management of credentials; (iv) knowledge and fear of risks; and (v) self-evaluation of security awareness. The study revealed that participants' confidence, their educational background, and parameters related to usability and accessibility significantly influenced their behaviour. For example, the ratios of users saving their credentials to stay logged in were 40.3%, 30.8%, and 48.6% for general, medium, and high smartphone competency levels, respectively.

3.3.2.2 Controlled Experiments Approach

The second approach is measuring security awareness using action-based research (other studies call it objective data sources). This approach tends to measure the actual behaviour through installing an agent and allows the researcher to monitor the participants' reactions to a specific security phenomenon. A few studies fall into this category. A study by Struse et al. in 2012 [58] investigated the security awareness of smartphone users regarding apps permissions. The study utilised a survey (of 113 participants) and found that more than 33% were not able to correctly identify the meaning of the permission for Full Internet Access. Further, the study developed an Android app (PermissionWatcher), which analyses the permissions of other applications installed on the mobile phone. The app was installed by over 1000 users and relied on a custom set of rules that classifies applications as suspicious if any rules apply. As a result, suspicious apps that require further actions by the users are displayed. The study concluded that users are willing to adhere to security principles whenever security awareness is created, and information is presented clearly and comprehensively.

A study published in 2015 by Wijesekera et al. [59] investigated Android app permissions to examine users' ability to deny applications access to the protected resources. The study was conducted through an experiment followed by an exit survey of 36 participants. A modification was done for the participants Android devices to log in whenever an application accessed a permission-protected resource. The study found that participants wanted to block a third of the permission requests. Their decisions were governed primarily by two factors: whether they had privacy concerns surrounding the specific data type and whether they understood why the application needed it. However, this study was very specific to permissions and did not cover other security aspects. A study by Felt et al. in 2012 [57] investigated Android users' awareness of frequently requested permissions. It focused on evaluating whether Android users pay attention to, understand, and act on permission information during installation. The study conducted two usability studies: an internet survey of 308 Android users, and a laboratory study in which 25 participants were interviewed and observed. The study results indicated that the majority of the participants displayed low attention and comprehension rates. Both the survey and laboratory study found that 17% of participants paid attention to permissions during installation, but only 3% of survey respondents could correctly answer all three permission comprehension questions. However, a minority of participants showed both awareness of permission warnings and reasonable rates of comprehension. The findings indicated that Android permission warnings did not help most users make correct security decisions.

A recent study published in 2020 by Bitton et al. [54] aimed to measure information security awareness of smartphone users for specific attack classes. The study measured the actual behaviour using a mobile agent and network traffic monitor and compared the findings with self-reported behaviour, which had been collected through a survey. The study involved 162 participants and found that their self-reported behaviour differs significantly from their actual behaviour. In addition, the information about the security awareness level derived from participants' actual behaviour was highly correlated with their ability to mitigate social engineering attacks. A study by Barth et al. in 2019 [55] tested the privacy paradox to focus on the actual behaviour, eliminating the effects of a lack of technical knowledge, privacy awareness, and financial resources. The study was conducted as an experiment (including a questionnaire) to evaluate the behaviour of end-users (66 participants) when downloading and using apps. Participants were university students with a decent technical background (i.e., they were Computer science students), and provided them with sufficient money to buy a paid app. The findings suggest that neither technical knowledge and privacy awareness nor financial considerations affect the paradoxical behaviour observed in users in general. Technically-skilled and financially independent users risked potential privacy intrusions despite their awareness of potential risks. The study found that participants did not rank privacy and security related aspects as important when downloading or using apps. Functionality, app design, and costs seem to play a major role in the downloading decision, although participants indicated earlier in the study survey that usefulness, functionality and trust, in particular, influence their app choice.

A study by Egelman et al. published in 2016 [56] aimed to measure computer and mobile device security attitudes of users by utilising the Security Behaviour Intentions Scale (SeBIS). Four main security sub-scales were investigated including awareness about phishing attacks, passwords, frequent updates, and locking the devices. The study was conducted through two surveys (555 participants) and a field study by utilising PhoneLab to monitor the security activities of 71 participants. The study found that: (i) testing high on the awareness sub-scale correlated with correctly identifying a phishing website, (ii) testing high on the passwords sub-scale correlated with creating passwords that could not be quickly cracked, (iii) testing high on the updating sub-scale correlated with applying software updates, and (v) testing high on the securement sub-scale correlated with smartphone lock screen usage (e.g., PINs).

We now present a conclusive summary and comparative analysis of the most relevant existing research, as in Table 3.5. Comparative analysis is based on four-point criteria including (i) *research challenge(s)*, (ii) *focus and contributions*, (iii) *evaluation context*, and (iv) *research limitations*. The study reference points to an individual research work under discussion and its year of publication.

Table 3.5 Comparative Analysis of most Relevant Existing Studies Compared to the Study Presented in Chapter 7

Study Reference	Research Challenges	Focus and Contributions	Evaluation Context	Research Limitations	Pub. Year
Survey-based Studies					
[40]	To exploit the Human Aspects of the Information Security (HAIS) model to investigate the security awareness of end-users regarding the usage of mHealth apps.	- Analyse end-users' security knowledge, attitude, and behaviour towards mHealth apps Investigate prominent security issues for end-users such as privacy and usability.	- Survey of mHealth app users (101 participants) Quantitative data	- Bias in data collection (diversity and types of participants) Self-reported behaviour by end-users	2020
[124]	To investigate, through empirical study, the security awareness of public institution personnel towards using mobile devices.	- Investigate Security habits of end-users (*apps' permissions, usage of antivirus and protection mechanisms, lock screen, etc.*)	- Survey of workspace users (120 participants) - Quantitative data	- Bias in data collection - Self-reported intentions of end-users	2019
[125]	To analyse the usage of security settings and control by mobile device users.	- Analyse security recommendations to users (e.g., *device settings, user behaviours, and applications)*	- Survey of mobile app users (94 participants) - Survey-based qualitative data. Quantitative data	- Bias in data collection (self-reported behaviour of users) - Diversity of users (i.e., students, faculty, and staff of one institute)	2017
[123]	To conduct an empirical Investigation into the cyber security awareness of end-users	- Analyse challenges of cyber security. - Investigate cyber security awareness (*cyber security practices, cybercrime awareness,* and *incident reporting.)*	- User survey questionnaire(629 users) Quantitative and qualitative data	- Data collected from end-users of mobile and PCs. Bias in data collection (self-reported intention)	2016
Controlled Experiments					
[55]	To investigate the privacy and security paradox of mobile users by focusing on the actual behaviour.	The study eliminated the effects (i.e., *lack of technical knowledge, privacy awareness, and financial resources).*	Experiment and survey (66 participants)	- Bias in recruiting users (High knowledge in IT). App selection might affect participants' consideration of security and privacy.	2019
[54]	To classify types of security threats and investigate information security awareness of mobile users for different classes of threats.	- Measuring security awareness of users - Measuring users' behaviour by mobile agent and network traffic monitor	- Survey of the mobile user (162 participants) - Monitoring of mobile agents and mobile network traffic	- No specific type of apps to be investigated	2020

[56]	To exploit the Security Behaviour Intentions Scale (SeBIS) to analyse the security attitudes of users	- Analyse the security attitude of users - Supporting users' security knowledge (e.g., awareness *of phishing attacks, frequent updates, passwords*, and *device locking*).	- User survey questionnaire (555 participants) Experimental monitoring of users (71 participants).	- No specific type of apps to be investigated Bias in data collection (creating passwords for low-risk accounts)	2016
Proposed Study in Chapter 7	To monitor the security awareness of end-users of mHealth apps via a security attack simulation.	- Understanding users' security behaviour when they are facing certain security threats/attacks.	- Utilising a simulation system and a survey to collect data. Quantitative and qualitative data	- Focusing on mHealth apps. - Multiple data sources (i.e., simulation-based, survey) Engaging end-users with diverse backgrounds (e.g., age, education level, etc.).	NA

Based on the presented studies in this section and the conclusive summary presented in Table 3.5, to the best of our knowledge, there has been no experimental research study to measure end-users' security awareness about using mHealth apps. This study aimed to investigate the security awareness of end-users of mHealth apps via an attack simulation approach. This approach investigated end-users' reactions by posing a few security threats and monitoring their spontaneous reactions. Such an investigation has helped us to understand and distinguish between self-reported behaviours and the actual behaviour. Furthermore, this study was followed by an exit survey to collect qualitative data from the participants and capture their security views.

3.4 Conclusions

The review (presented in Section 3.1) was motivated by the growing amount of attention to mobile apps, particularly mHealth apps. We aimed to analyse and synthesize the literature to identify the challenges that hinder mHealth apps' developers from developing secure apps. Our review followed an SLR approach and selected 32 studies that we believe are relevant to our study. We have identified and discussed nine challenges faced by mHealth apps developers to develop secure apps. We also provided a conceptual framework for the identified challenges as well as presented a number of challenges linked to the body of knowledge found in this literature review. Our findings can be valuable for researchers and practitioners (e.g., mHealth app developers, managers) to support the research and development of secure mHealth apps. For researchers, this review would help to identify the existing research that would support formulating and testing hypotheses. Furthermore, proposing ideal and innovative solutions to address these challenges. For practitioners, our review would help to understand the existing challenges of developing secure mHealth apps from the literature. This would help to resolve these challenges at the early stages of the mHealth apps development process.

Smartphones provide many benefits due to their sophisticated characteristics and features. Most of the tasks can be done through mobile apps which have been specifically developed for certain purposes. mHealth apps enable data collection and transmitting them to health provider systems. However, security becomes an important element and a major challenge that requires attention. Successful implementation of mHealth apps necessitates sufficient security features to be employed by the developers, and awareness and knowledge of the security from the end-users' side. End-users' level of security awareness and knowledge have a significant impact on security by helping them to avoid severe consequences (e.g., sharing private health data unintentionally with a third-party app). The review (presented in Section 3.2) aimed to understand the security concerns and issues of using mHealth app by focusing on end-users views. The review provided the knowledge for expanding the research and conducting further studies regarding end-users' security awareness about mHealth apps.

Simultaneously raising the security awareness of mobile end-users is very important due to the high number of security threats and the numerous malicious activities. Such an awareness would help to secure confidential data stored within the devices. However, the level of security awareness for end-users of mobile apps has not been given enough attention and is often forgotten, especially in real-life scenarios. End-users' security behaviour is the key to ensure that health data within their devices are secure. A review of the literature was conducted (presented in Section 3.3) to understand the existing mechanisms to measure the security awareness of end-users of mobile apps. The review helped to design the study protocol (Section 2.4.1) for measuring the security awareness of end-users of mHealth apps.

Chapter 4

Challenges, Practices and Motivations to Develop Secure mHealth Apps

Related publication:

This chapter is based on APSEC 2020 paper titled "An Empirical Study on Developing Secure Mobile Health Apps: The Developers' Perspective" [34].

In Chapter 3 (Section 3.1), we noticed that studies have pointed out some security challenges that hinder the developers to develop secure mHealth apps. However, there is no empirical study, to date, that fully focused on investigating this matter. This chapter aims to empirically investigate the challenges that prevent the developers to implement security in mHealth apps (RQ2: What are the challenges that developers of mHealth apps face with respect to implementing security? Section 4.4.1). In addition, we investigated the security practices and proposed a taxonomy (RQ3: What motivates mHealth apps developers to develop secure mHealth apps? Section 4.4.2). Also, motivational factors that may impact the developers to ensure security in mHealth apps have been explored (RQ4: What security practices are used to incorporate security measures in mHealth apps? Section 4.4.3). We conducted a survey questionnaire with 97 mHealth apps developers. The findings revealed 10 critical challenges such as lack of the required budget for implementing security during the development process of mHealth apps, and insufficient security knowledge for the developers, (ii) presented a taxonomy of the best practices to ensure security during SDLC, (iii) reported 10 motivational factors that impact secure mHealth apps such as vision and reputation of organization, and security team leads to influence secure SDLC. Our results highlight potential areas for future research and provide evidence-based for practitioners to ensure the security of mHealth apps.

4.1 Introduction

Mobile health apps empower healthcare stakeholders (i.e., medics, patients, etc.) to exploit embedded sensors of a device for health diagnostics such as monitoring body temperature, pulse rate, and blood pressure [15]. mHealth apps rely on the portability and context-sensitivity of mobile computing to improve access to healthcare services that are cost-effective, scalable, and pervasive [4]. World Health Organisation (WHO) has defined mHealth as *"medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices [12]"*. mHealth apps range from decision support for reproductive health to fitness monitoring apps for nutrition management [5]. The usage of mHealth apps by healthcare practitioners and patients is on the rise with 350000 such apps available in two app repositories provided by Android and iOS platforms [11].

Mobile apps in general and mHealth apps in particular collect, process, store, and transmit user and device data in and out of a device over various networks [5]. Typical examples of such apps are location services or a banking app that needs the device's type and ID, user's location and preferences to function properly [1, 127, 128]. Any compromise on the confidentiality, integrity, and availability of such data leads to severe consequences including but not limited to compromised devices, location and activity tracing, and financial loss. Therefore, the security of mobile apps is a critical concern for users (regarding data security) and app providers (to ensure secure app development) [70]. In the case of mHealth systems, the security of mobile apps becomes a significant concern due to the privacy and integrity of health-critical data [5, 29], as an attack can modify the blood pressure or pulse rate of a patient that has medical, legal, financial, and social consequences [16].

Existing research such as [1, 8, 15-17, 35] indicated that the security of mHealth apps lags behind the capabilities of adversaries and the sophistication of cyber-attacks that target the apps. A recent study suggests that despite their benefits, a wide spread adoption of mHealth apps is hindered due to users' concern about security and privacy of their personal and health-critical information [23]. To address such issues, it becomes vital to investigate the security of mHealth apps by incorporating practitioners' views on challenges, best practices, and motivations to ensure secure mHealth apps. Such an investigation can help us to understand and address some fundamental issues such as why mHealth apps are not secure, and what efforts could be made to make them secure. In this chapter, we investigate the security of mHealth apps based on developers'[5] view to understand (i) critical challenges that hinder the development of secure apps (ii) development practices to ensure the security of mHealth apps, and (iii) motivations for secure app development. We outline the Research Questions (RQs) as below:

RQ2: *What challenges do developers face while developing secure mHealth apps?*

RQ3: *What practices are used to incorporate security measures in mHealth apps?*

RQ4: *What practices are used to incorporate security measures in mHealth apps?*

We conducted a web-based survey that received responses from 97 app developers. Demography analysis of developers' data indicates their experiences, team size, and professional roles to develop mHealth apps for mobile platforms including Android, and iOS. To ensure the quality of responses, we only allowed developers with first-hand experience in developing mHealth apps to participate in our survey. The results can be beneficial for researchers and practitioners (e.g., mHealth app developers, managers, research engineers) to support the research and development of emerging and next generation of secure mHealth apps.

4.2 Related Work

We organised the related work in three themes (Section 4.2.1) security issues, (Section 4.2.2) development challenges, and (Section 4.2.3) developers' practices and motivations for secure app development.

4.2.1 Security Issues with Current mHealth Apps

A recent mapping study [30] of 365 papers on m/uhealth security and privacy highlights that the security and privacy specific education and training for developers are one of the critical factors to support secure development of mHealth systems. Some other studies have focused on investigating the security of mHealth apps by means of security experiments [15], static and dynamic analysis [1], comparative analysis [16], security assessment [17], and vulnerability scanning [8]. These studies revealed that most of the mHealth apps lack the incorporation of security countermeasures, such as access control and threat detection. For example, He et al. [35] revealed that several mHealth apps are prone to attacks due to inherent vulnerabilities such as transmitting mHealth data in unencrypted form and logging sensitive information. Moreover, numerous mHealth apps expose their security-critical components to adversaries and some apps store unencrypted information on external storage, e.g., SD Card, where a malicious app can read and modify it [35]. In [1], the authors have reported that mHealth apps developers may fail to appropriately implement even the basic security solutions such as authentication, access control, and data encryption that impacts security and privacy of health information.

4.2.2 Challenges to Develop Secure mHealth Apps

Through a systematic review [43], we identified that in order to ensure the security of mHealth apps throughout their development lifecycle, the developers need to be vigilant about security-related issues. Contrary to the finding of [43, 129], some studies highlight that the developer of mHealth apps are not

[5] The terms *developer*, *practitioner*, *respondent*, and *participant* have been used interchangeably in this paper all referring to professionals who are engaged with engineering and development of secure mHealth mobile apps.

even familiar with fundamental solutions such as security measures [8, 36], security tools [128], and trusted libraries [17, 130] that are critical for secure app development. Developing mHealth apps needs updated security knowledge, especially knowledge about integrating mHealth apps technologies that are driven by context-sensitive and pervasive computing enabled by mobile and the Internet of Things (IoT) [35]. It is vital to mention that the primary purpose of health and security regulations (e.g., Health Insurance Portability and Accountability Act -HIPAA) is to protect health-critical data and to promote trustworthy systems. However, such regulations do not provide explicit guidelines, processes, and methods to assist the stakeholders (e.g., users, developers, etc.) of mHealth apps [4, 29]. Moreover, frameworks and standards for developing secure mHealth apps are still missing from the existing regulations, policies, and development initiatives [1, 8, 16].

During software development, project-specific constraints such as time and cost to deliver, can pressurize developers to focus on satisfying functional specifications first and patching advanced security issues after the initial release [5, 36]. Patching security specifications in a released app is a costly approach and introduces new vulnerabilities after fixing the existing issues [15]. Also, the lack of security testing due to timing and financial constraints for mHealth apps development projects is a challenge that is reported in various studies [15, 36, 131]. Other issues such as absence of security experts, lack of understanding for security testing tools, and shortage of budget to conduct app testing are attributed as fundamental challenges for developing secure apps [43].

4.2.3 Developers' Practices and Motivations

A lack of adoption or poor understanding of security practices by mHealth apps developers' hinders the development process for secure software engineering [12]. The consequences of compromised security practices – during the software development lifecycle (SDLC) – makes apps vulnerable, such as permitting an app to share health-critical data with other mobile apps (e.g., untrusted apps or external hosts [4]). Thamilarasu et al. [36] examined the top 15 Android-based mHealth apps and found 248 vulnerabilities. The study identified that the top 3 vulnerabilities were caused by development practices that are followed by developers, e.g., selection of cipher method or implementation of specific algorithms to request or grant permissions. It concludes that most of these vulnerabilities could have been prevented by adopting development practices that adhere to secure SDLC.

Developers' and team motivation are two of the key success factors for software projects [97]. Many security incidents are primarily caused by human rather than system failures [98]. Motivational factors that help mobile apps developers to achieve security were discussed by Weir et al. in [85]. The study pinpointed that developers were motivated by their security knowledge and experience, considering security as a task that needs to be done in the right way, impacts of developing insecure software, and pursuing secure development as an enthusiasm. Developers motivation for secure software development when coupled with security specific education and training is among the most important factors for security of mHealth apps [43]. Reusing source code from a previous project is a common practice to promote reusability and cost-effectiveness; nevertheless, security bugs can be inherited by adopting such practices [8, 16, 17, 35]. Also, copying or reusing the source code from web-based public repositories (e.g., Stack Overflow (SO) or GitHub) without examining the code is a common practice among app developers that leads to developing vulnerable apps. The impact of copy/pasting of source code from SO to Android apps was investigated in [132]. The study revealed that 97.9% of the copy/pasted code contained at least one insecure code snippet.

It should be noted that none of the above-mentioned studies has empirically investigated the challenges, practices, and motivations for developing secure mHealth apps based on the developers' perspectives. Our study provides an empirical basis for the development practices that enable or enhance secure app development for mHealth systems.

4.3 Research Method

In this chapter, we used a survey questionnaire, which is detailed in Chapter 2, Section 2.2. The findings of this chapter are based on surveying 97 mHealth apps developers.

4.4 Findings

We now present the findings of the survey to answer to outlined RQs. Answers to the RQs are presented in the dedicated sections as: (i) *security challenges* (**RQ2**) in Section 4.4.1, (ii) *development practices* (**RQ3**) in Section 4.4.2, and (iii) *motivating factors* (**RQ4**) in Section 4.4.3. Section 4.5 consolidates the overall findings of the study by highlighting key results for all RQs, their limitations, and needs for future research.

4.4.1 Challenges for Secure mHealth App Development (RQ2)

In order to identify the challenges faced by developers, i.e., answer to RQ2, we formulated eight Security Challenge statements, (**SC1** to **SC8**) based on the findings and guidelines of our SLR [43]. The statements capture the input of 97 Respondents (**R1** to **R97**). For an objective interpretation and assessment, we sought developers' feedback on each statement using a five-scale Likert (*Strongly Agree*, *Agree*, *Not Sure*, *Disagree*, and *Strongly Disagree*) as in Figure 4.1. Furthermore, the responses to these statements were complemented by an open-ended question that allowed developers to spontaneously share other challenges based on their knowledge and experience. The results of developers' perspectives on each of the 8 challenges are detailed below.

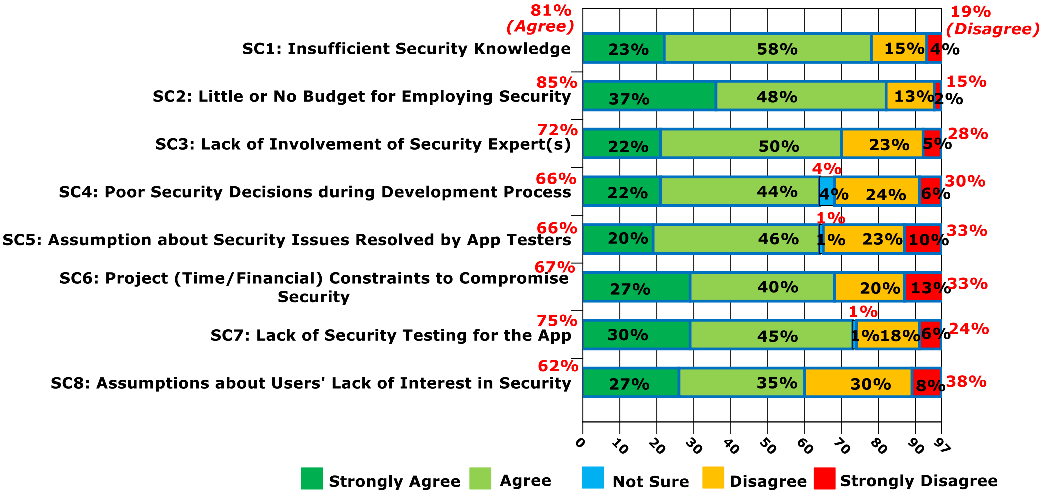


Figure 4.1 Responses for Critical Challenges Related to Security of mHealth Apps

SC1) Insufficient security knowledge of the developers: Developing secure mHealth apps require proper security knowledge. Typical examples of security knowledge include but are not limited to coding practices, robust usage of security testing tools, and confidence in using third-party libraries that should be known by mHealth apps developers [43, 129]. We asked the respondents to rate their agreement or disagreement while considering insufficient security knowledge as a challenge for developing secure mHealth apps. While 19% of the respondents disagreed, 81% of them affirmed that inadequate security knowledge is a challenge for mHealth app development reflected as SC1 in Figure 4.1. Some respondents elaborated that poor skills for secure programming is a critical challenge to develop secure apps. It was highlighted that mHealth apps developers face difficulties in using programming tools and reusing code that can be vulnerable. For example, as per the claims of **R13** and **R45** *"Cloning of certain features by other developers"* and *"Picking up code written by the hacker represents a critical challenge"*. Some respondents pointed out that they have a lack of security knowledge in dealing with attacks and vulnerabilities. Specifically, **R59** shared that *"[him/her] not being aware of potential security risks"* and **R46** emphasized that *"mHealth apps developers need to put more effort to enhance their security knowledge through R&D and learning new technologies"*.

SC2) Little or no budget for employing security: Developing secure software requires allocating a specific budget to be spent on enhancing the security of developed and deployed apps [43]. Such a budget would help to support secure mHealth apps development. For example, allocating a sufficient budget would provide the security tools which can be used to test the app during development. Not to mention security tools can be expensive and requires investing in training the developers on how to use them. Furthermore, performing penetration testing for the developed mHealth app requires hiring a third-party organization, which can bring extra cost. Thus, we asked our respondents to rate their agreement or disagreement with SC2, i.e., little or no budget for employing security. 85% of them affirmed that developing secure mHealth apps cannot be achieved without assigning an adequate budget. Only 15% disagreed with the statement SC2 in Figure 4.1. Our analysis of the responses revealed that lack of allocated budget for secure mHealth apps represents the most critical challenge.

SC3) Lack of involvement of security experts during software development: The absence of security experts is being recognised as a factor that directly influences secure software development [73]. Involving security experts during apps development would give inexperienced developers access to the required security knowledge (SC1) [43]. We asked our respondents if they consider the lack of security experts' involvement during the development as a challenge, as SC3 in Figure 4.1. Given the responses, 72% of participants indicated that their mHealth app development teams lacked security experts; whereas 28% of them disagreed with this statement. We looked into the experiences of the respondents, who showed their disagreement from Figure 2.2 (d) and data in [45]. We found that the majority of the respondents (20/27 developers, i.e., 74%) have more than 5 years of experience in developing mHealth apps. Hence, they depend on their ability and expertise in developing secure mHealth apps without relying on security experts.

SC4) Poor security decisions during the development process: Developing mHealth apps requires making appropriate security decisions with respect to storing and using health-critical data [98, 132]. Poor security decisions during mHealth apps development would leave mHealth apps vulnerable to security threats. Besides, the high cost of fixing flaws (e.g., security patching [5]), mHealth apps development organisation may face technical and legal issues for the data breach. Thus, mHealth apps developers' and their organisations need to pay careful attention to security-related decisions. We asked respondents about their views on security decisions during the development process, SC4 in Figure 4.1. 66% agreed that making poor security decisions during the SDLC is a challenge, while 30% disagreed with this statement. Only 4% of our respondents were neutral.

SC5) Assumption about security issues resolved by app testers: Ensuring security is a task that needs to be considered by software developers throughout the SDLC. However, Xie et al. in [100] concluded that one of the main reasons that lead software developers to make security errors is relying on others, such as app testers or independent reviewers of source code. In fact, 66% of respondents agreed that app testers should make decisions about ignoring or identifying security flaws. 33% disagreed and only 1% were neutral, as SC5 in Figure 4.1.

SC6) Project constraints to compromise security: Project constraints, specifically time to deliver and cost efficiency (SC2), represent common challenges for software engineering projects as well as for SDLC of secure mHealth apps [73]. Time to deliver – relative to market competition – forces development teams and developers to primarily focus on functional requirements and often overlook or ignore quality requirements that include security features. According to our respondents, 67% of them agreed that meeting app development deadlines pressurizes developers to compromise security requirements and their testing. 33% disagreed with this statement SC6 in Figure 4.1. Respondents including **R12**, **R37**, **R50**, **R58**, and **R62**, commented that it is a challenge to ensure the security of mHealth apps due to time constraints. **R62** claimed that *"Lack of time for app delivery stresses developers that impacts quality specific requirements such a security, performance, scalability and many more in secure [mHealth] app project deadlines is a significant challenge for developers"*.

SC7) Lack of security testing: Security specific testing is a crucial phase throughout SDLC to identify potential vulnerabilities in the security and privacy of the developed app. In the context of mHealth apps, it helps to address security threats, such as unauthorised access to health data, tampering with health data or reporting invalid data to health providers. We asked our respondents if they consider lack of security testing as a challenge to develop secure mHealth apps. While 75% of respondents agreed with this statement, 24% indicated their disagreement and 1% were neutral for SC7 in Figure 4.1. Five respondents **R38**, **R45**, **R52**, **R62**, and **R95** commented that the lack of rigorous testing for mHealth apps is the most critical challenge for them.

SC8) Assuming that users are not that much interested in security: Security should be incorporated and addressed ideally throughout the SDLC from requirement analysis to the deployment phase [91].

Incorporating security at later phases of software development or after release in the form of security patches can be costly exercise and can introduce new vulnerabilities [133]. However, the trade-offs between security and other quality attributes such as usability and performance can be problematic. R27 and **R63** indicated that app accuracy and performance are challenges that affect the development of secure mHealth apps. Consequently, developers might assume that users are not concerned about security and hence lowering the priority given to security due to budgeting or time constraints. 62% of the respondents agreed that users are not interested in security. 38% disagreed as per SC8 in Figure 4.1. Four respondents **R54**, **R62**, **R73**, **R81** indicated that mHealth apps developers' pay little or no attention to security. **R62** stated that *"We are yet to be engaged in a mobile health project where we put specific focus on security aspects of the app"*. **R54** claimed that *"There [are] very few developers in my community who bother about security"*, and **R73** indicated that *"I think a large number of the other players in the space don't take it seriously enough. I think they aren't paranoid enough"*.

Other Challenges (Open-ended): In addition to close-ended statements from **SC1** to **SC8**, the respondents highlighted 'other' challenges, detailed below, they see as important but were not presented as survey questions.

a) Dealing with legal obligations, policies and procedures: mHealth apps can be classified as low-risk apps (e.g., fitness apps) and high-risk apps (e.g., clinical decision-support apps) [134]. Given the criticality and confidentiality of health-critical data, various governments have established different compliances such as HIPAA to ensure security and privacy. In this context, **R39** and **R57** highlighted that policies and regulations for mHealth app development are ideal but complex to implement and abide by. **R9**, **R55**, **R60**, **R72**, **R91** found lack of guidelines, documentation, and better procedures to ensure app security.

b) Challenges of maintaining mHealth app and data: Six respondents **R16**, **R29**, **R43**, **R57**, **R86**, **R92** indicated that there are difficulties in maintaining mHealth apps and data due to the complexity and privacy-preserving nature of data. Specifically, **R16** stated that maintaining mHealth apps requires proper security management team. **R57** suggested keeping third party libraries updated to avoid any security vulnerabilities from code execution. **R29** pointed out that *"continuous updates [are needed] so that you don't miss any new medications or information"*. **R43** and **R92** mentioned that mobile phone and platform compatibility (e.g., Android, iOS etc. platforms) is a challenge in maintaining mHealth apps with **R82** indicating that *"Privacy preservation of the data collected by the app"* is the most critical challenge.

4.4.2 Practices to Ensure Security of mHealth Apps (RQ3)

In order to identify the developers' practices, i.e., finding an answer to *RQ3*, we explored how security-specific development practices are integrated during the mHealth apps development process by our respondents. We used open-ended questions because we did not want to limit our respondents while sharing the practices they adopt and their relative experiences [29]. Although there are several guidelines for Secure Development Lifecycle such as [92], we used Microsoft secure software development process (having five development tasks) to analyse and document the provided responses by the developers. Based on the developers' responses, we created a taxonomy of the development practices in Figure 4.2 to classify the specific practices that ensure security during each task of the SDLC. The taxonomy in Figure 4.2 also helps with conceptualisation and quick identification of all the practices that developers perceive as effective to enable or enhance app security.

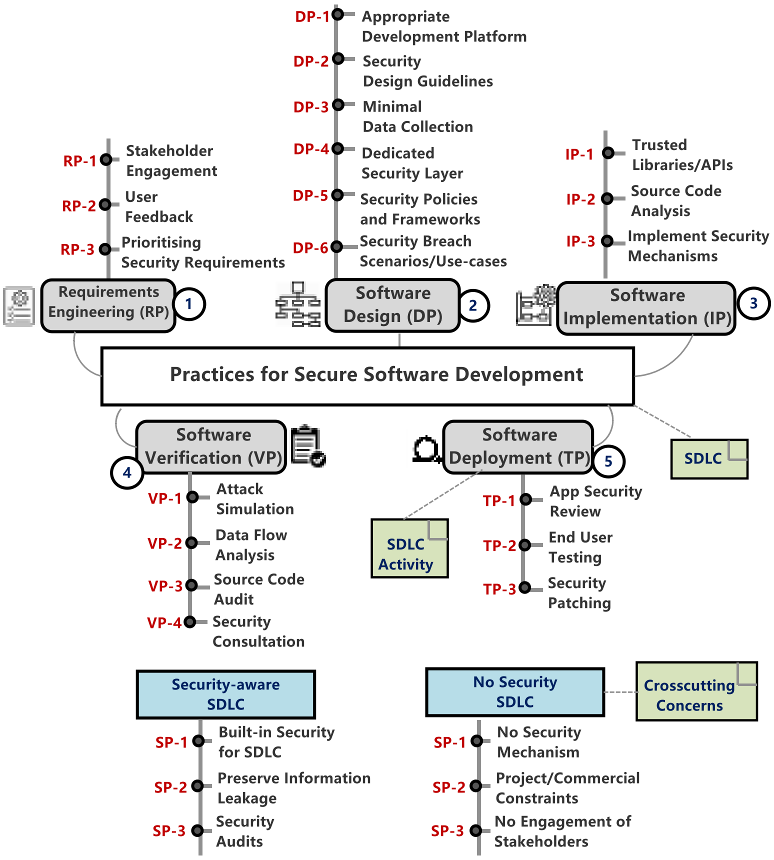

DP-1 Appropriate Development Platform
DP-2 Security Design Guidelines
DP-3 Minimal Data Collection
DP-4 Dedicated Security Layer
DP-5 Security Policies and Frameworks
DP-6 Security Breach Scenarios/Use-cases
RP-1 Stakeholder Engagement
RP-2 User Feedback
RP-3 Prioritising Security Requirements
IP-1 Trusted Libraries/APIs
IP-2 Source Code Analysis
IP-3 Implement Security Mechanisms
Requirements Engineering (RP) 1
Software Design (DP) 2
Software Implementation (IP) 3
Practices for Secure Software Development
Software Verification (VP) 4
Software Deployment (TP) 5
SDLC
SDLC Activity
VP-1 Attack Simulation
VP-2 Data Flow Analysis
VP-3 Source Code Audit
VP-4 Security Consultation
TP-1 App Security Review
TP-2 End User Testing
TP-3 Security Patching
Security-aware SDLC
No Security SDLC
Crosscutting Concerns
SP-1 Built-in Security for SDLC
SP-2 Preserve Information Leakage
SP-3 Security Audits
SP-1 No Security Mechanism
SP-2 Project/Commercial Constraints
SP-3 No Engagement of Stakeholders

Figure 4.2 Taxonomy of Development Practices for Secure mHealth Apps

4.4.2.1 Task I – Requirements Engineering

As the initial task of SDLC, requirements engineering involves identifying, specifying, managing, and implementing security requirements for the app to be developed. Engaging stakeholders in security requirement engineering is being recognised as a key to software success, as well as getting effective outcomes. In Section 4.2.2 (SC4, Figure 4.1), we reported that poor security decisions could be caused by lack of stakeholders' involvement in SDLC. Three respondents identified as **R60**, **R78**, **R96** indicated that they involve users feedback and try to negotiate requirements with users as an approach to employing security during requirements engineering. For example, respondent **R78** claimed that *"In my case, it [requirements engineering] involved discussing requirements and what would be the most sensible solution to ensure security requirements"*.

4.4.2.2 Task II – Software Design

This task is essential to represent the identified security as a design or blueprint of the software to be implemented. **R45**, and **R60** indicated that selecting the right development platform and supporting tools would help to enhance the security of mHealth apps. Four respondents **R28**, **R60**, **R82**, **R85** mentioned that adhering to security guidelines helps ensure security of mHealth apps. **R45** and **R48** pointed out that as a design consideration, minimising data collection, sharing and asking for personal information positively impacts security of mHealth apps. **R51** and **R52** indicated that they ensure the security of mHealth apps through utilising a layered approach (incorporating a dedicated security layer) and secure data storage. Also, using security frameworks, standards along with policies would help to design secure mHealth apps and comply with security regulations. Furthermore, **R57** and **R72** indicated that they analyse and map the attack surface, specifically **R72** claimed that *"Thinking about all ways where hackers could be intrusive can help design possible scenarios to countermeasure security breaches"*.

4.4.2.3 Task III – Software Implementation

This task of SDLC is about writing the source code to implement the design (from Task II) based on the identified security requirements (as in Task I). App implementation focuses on coding/implementing security measures (e.g., encryption, anonymization) into apps. **R57** and **R74** indicated using trusted libraries or APIs as a best practice to ensure the security of mHealth apps. **R57** suggested that he is

"Following industry specific [code libraries, APIs] practices rather writing custom source code to ensure app security". **R74** claimed that *"[…], we [as part of development team] just do basic AES encryption of user data"*. **R30** and **R38** mentioned that they utilise static analysis [1] of source code as part of the implementation task to ensure security.

4.4.2.4 Task IV – Software Verification

It aims to analyse the implemented app (in Task III) and identify potential flaws that can be exploited for malicious access. As part of software verification, app testing is an effective approach to determine security vulnerabilities and threats, thus, employing suitable measures [5, 29]. Analysing the responses, we found that 16 respondents have indicated app testing as their best practice to ensure security. Specifically, app testing involves practices such as attack simulation, data flow testing, code review, and penetration tests. **R86** mentioned that, "Testing app vulnerabilities by simulating attacks is an effective practice to assess security strength of the application". **R84** and **R90** mentioned that they conduct data specific testing (e.g., data leakage testing, data encryption testing). **R83** and **R97** mentioned internal code review as a proven practice to test the security strength of their apps. **R83** suggested, *"Multiple people to review source code [can avoid potential bias of code inspection]"*. Five respondents **R9**, **R39**, **R57**, **R73**, **R89** indicated that they performed testing with external security experts. **R9** mentioned *"Hiring a computer security firm to run penetration tests"*, and **R89** suggested, *"Invite third-party companies for security audit and testing"*.

4.4.2.5 Task V – Software Deployment

As the last task of SDLC, it refers to the release and deployment of the app to be used by users. One respondent, **R37**, indicated that they perform a final security review to ensure the security of mHealth apps. Respondent, **R4**, believed that most of the developers are only able to fix security flaws after deployment and user testing. **R4** claimed that, *"[in our team] we found that most of our peers approach security testing during deployment, once the system is operational"*.

Furthermore, automatic vulnerability patching is a method to ensure the security of mHealth apps. The responses from the participants regarding security practices suggested:

a) Security-aware SDLC: Considering security throughout SDLC represents an ideal practice to develop secure software. This practice not only ensures incremental security (from requirements to deployment) but also reduces the cost and efforts of fixing security errors afterwards in the form of security patches. Five respondents **R26**, **R55**, **R73**, **R74**, and **R85** indicated that throughout the SDLC satisfying the security requirements of mHealth apps remain their primary concern. **R74** suggested that *"[Development] should be more concerned about security before as cyber attacks frequency increases"*, and **R26** suggested, *"Preserving user personal information from any leakage is ultimate success for any secure development process"*. Also, **R39** and **R57** indicated that they consult security experts throughout SDLC.

b) No security approach is being considered: While security becomes an important concern during SDLC, yet according to a few respondents, it is still not much of a concern to them. Four respondents **R62**, **R70**, **R71**, **R81** indicated that they did not follow any approach to address security during the development process. **R61** claimed that *"We are yet to be engaged in a mobile health project where we paid specific focus to the security aspect"*, and **R70** claimed that *"No process most of the time. Development teams [due to project constraints and commercial reasons] have no direct link with medical teams (stakeholders), and due to this lack of interaction, user are using apps that can be disastrous for security and privacy of mHealth data"*.

4.4.3 Motivations to Ensure Secure App Development (RQ4)

To identify the motivating factors for secure mHealth app development, i.e., to answer ***RQ4***, we formulated six Security motivation statements (**SM1** to **SM6**) based on the findings and guidelines of our SLR [43]. The statements capture the responses of 97 respondents (**R1** to **R97**) as illustrated in Figure 4.3. To objectively interpret and assess the responses, we sought developers' feedback on each statement using a five-scale Likert (Strongly Agree, Agree, Not Sure, Disagree, and Strongly Disagree) as in Figure 4.3. In addition, input to these statements was complemented by an open-ended question to allow developers to share other motivating factors based on their knowledge and experience.

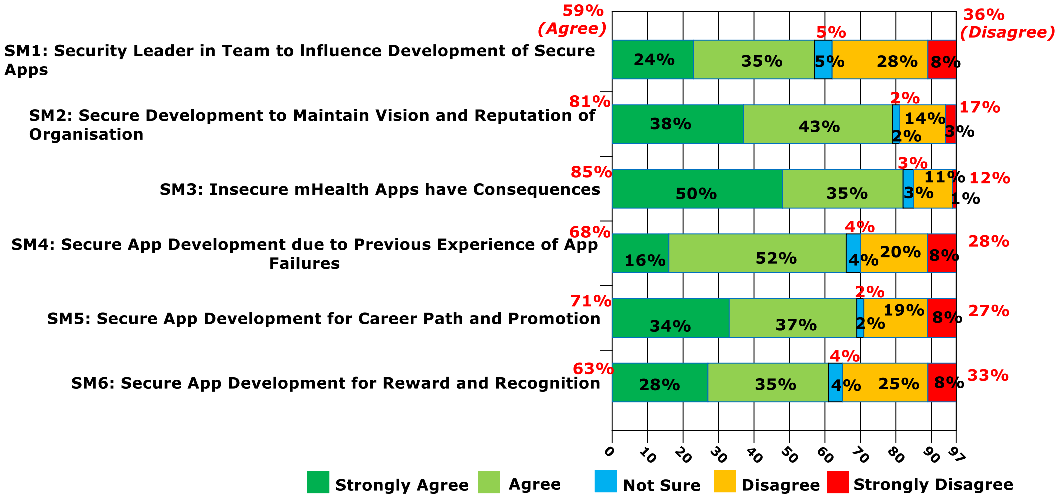


Figure 4.3 Responses for Developers' Motivations to Develop Secure mHealth Apps

SM1) Security leader in the team to influence the development of secure mHealth apps: Commitment to improving the security is one of the main goals that security team leads aim to achieve. The respondents **R2** and **R38** indicated that they follow security experts' comments and guidelines to ensure security. Specifically, **R2** claimed that *"Following security department feedback is required during the design"*, and **R38** suggested that *"[...] and following the guidelines of Security Expert"*. 59% of the respondents agreed that a security specialist as team leader influences and motivates them to develop secure mHealth apps. 36% disagreed and 5% remained neutral on the role of security leaders in the team indicated as SM1 in Figure 4.3.

SM2) Secure development to maintain vision and reputation of the organisation: Creating and maintaining the reputation is a common goal that software development organisations seek to fulfil their vision. **R45**, **R69**, **R91** emphasised that they consider maintaining the organisation's reputation along with building trust and credibility as their motivations to develop secure mHealth apps. **R45** claimed that *"[…] and the second thing is by developing a secure application, the client's trust will become strong"*. Satisfying end users can help to maintain the organisation's reputation and fulfil its vision. Four respondents **R27**, **R61**, **R72**, **R92** commented that patients' expectation, users' expectations and satisfaction are their motivations. One respondent mentioned that developing secure mHealth apps also proves the organisation's proficiency to deliver security-enabled software. **R4** claimed that, *"I develop secure applications, and share our experience, so we can grow a stronger development community within our local market"*. In fact, 81% of the respondents agreed that maintaining the reputation of their organisation is a motivation for developing secure mHealth apps. While 17% disagreed, only 2% were neutral to the statement SM2 in Figure 4.3.

SM3) Insecure mHealth apps have consequences: Monitoring patients' health, sending data to health providers, and receiving health professional decisions is one of the central features of mHealth apps. The consequence of tampered data by unauthorised entities can be damaging. Considering the consequences of insecure mHealth apps on patients' personal and health-critical information received the highest mutual agreement among the respondents. 85% of the respondents (i.e., 82 out of 97 with 50% as strongly agreed and 35% as agreed) affirmed that mHealth apps suffer from negative comments and user dissatisfaction if they are insecure. Only 12% disagreed and 3% remained neutral as SM3 in Figure 4.3. Respondents emphasized that the safety and privacy of patients' data is their motivation to ensure the security of mHealth apps. Specifically, **R93** claimed that *"[…] and ensuring safety is our principle and bottom line"* and **R97** claimed that, *"[…], I care more about their safety"*. Two respondents **R73**, and **R77** indicated that avoiding health data leakage is their motivation for security.

SM4) Secure app development due to previous experience of app failure: We also wanted to examine the motivation for secure app development due to past experiences of app failure(s). 68% of the respondents agreed that they had experienced application failure in the past. Thus, it became their motivation to ensure security for the apps that they develop and specifically for mHealth apps. 28% disagreed with this statement and 4% of the respondents were neutral as SM4 in Figure 4.3.

SM5) Secure app development for career path and promotion: Despite the overwhelming challenges of developing secure mHealth apps, some developers pursue the development of secure mHealth apps as an ambitious activity for the sake of their interests and ambition. Three respondents, **R30**, **R47**, and **R63**, pointed out that personal interest, such as continuous learning and promotion is their motivations to ensure security. For example, **R47** stated that *"[I] Keep learning to improve skills [for security aware app development]"*. 71% of the respondents affirmed that they develop secure mHealth apps because they look for career path and promotion with skills and expertise in software security and secure app development in particular. 27% disagreed and 2% were neutral about SM5 in Figure 4.3.

SM6: Secure app development for reward and recognition: It is considered by developers as personal achievements in terms of financial or other gains that help them advance their development portfolio and profile (relevant to SM5). Expecting a reward and recognition was a motivation for developing secure mHealth apps for 63% of the respondents who agreed with SM6 in Figure 4.3. 33% disagreed and 4% were neutral that reward and recognition is a motivation for them to do secure app development.

Other Motivations (Open-ended): Respondents were asked about 'other' motivating factors they see as critical but were not presented in the survey questions.

a) Organisational practices for ensuring security: Developing secure mHealth apps cannot be achieved without organisational commitment such as providing sufficient security tools, engaging mHealth apps developers in security training, and employing security team leads [43]. Such a commitment helps to overcome the challenges, also mentioned in Section 4.4.1. More importantly, it would strengthen the security culture of mHealth apps developers' and their motivations to ensure security. Our respondents provided us with several responses indicating that their organisations are committed to security. **R38** indicated that proper quality assurance and testing is a motivation to develop secure mHealth apps. Respondents **R31** and **R33** mentioned that they were motivated by utilising security tools which provided to them by their organisation.

b) Ethical obligations: Software development is an intellectual and effort intensive process which can be influenced by developers' behaviour. Also, mHealth apps developers' behaviour can affect their security practices (e.g., making a decision to use a third-party service to process users' data), and thus, impacting the security of an app. Thus, incorporating the ethical perspective is a key to motivate mHealth apps developers' to ensure security. 11 respondents **R19**, **R26**, **R37**, **R43**, **R45**, **R55**, **R59**, **R68**, **R88**, **R95**, **R96** believed that ensuring security is part of their ethical obligations. **R37**, **R43**, and **R96** indicated that they were responsible for the security of their apps. **R37** claimed that, "*Just to help everyone if I do not do my job, why would I get paid?*", and **R45** suggested, "*The main factor which motivates me to develop secure mobile health apps is that, we need to keep in mind the security of the data which a user allows to share with the application and it's duty of the development organisation to keep that data private and secure that no one can misuse the data*".

c) Legal obligations: Developers of mHealth apps should take into consideration the safety and privacy of their users as well as complying with laws and regulations. **R3**, **R39**, **R48** indicated that legal liability or its consequences are primary motivations to ensure security. Underestimating security can lead to breaches of policies and regulations resulting in governmental fines for data breaches. Failure to secure patients' data could result in legal liability against the development organisations. **R3** indicated, "*I develop a secure mobile application because I know if any PHI [Personal Health Information] has been leaked, my organisation has to pay millions of dollars*".

d) Reducing the cost of maintaining the app: Fixing security errors after developing mHealth apps can be error-prone, costly, and time-consuming [133]. Reducing the cost of app maintenance was perceived as a motivation to ensure the security of mHealth apps, responded by **R40**.

4.5 Discussion of Results and Future Work

We now discuss the key results for the investigated RQs (i.e., ***RQ2***, ***RQ3***, ***RQ4***) and highlight possible future research that extends the findings of this study.

4.5.1 Challenges for Secure mHealth App Development

– Budget for security in SDLC: Developers' perspective (i.e., 85% of respondents as in Figure 4.1) highlighted that allocating little or no budget to support security-specific activities in SDLC is a major concern for mHealth apps. Hence, ensuring the security of mHealth apps necessitates assigning the required budget that can be used to hire security experts who can manage all security concerns, or adopting security tools that also require training the developers to ensure proper utilisation.

– Insufficient security knowledge: Knowledge of security mechanisms and implementations in development teams or at the organisation level hinders the development of secure mHealth apps, responded by 81% of the developers. Management support for the developers during apps development is extremely important to ensure functional as well as quality specific requirements that are related to the security of mHealth apps.

Needs for future research: Our analysis of the security challenges for mHealth apps pinpointed the need to go beyond developers' views to also collect and analyse users' knowledge, perception, and interests regarding security and privacy of their data. As part of future work, we aim to conduct users' survey that can unveil security challenges from their perspectives (i.e., users of mHealth apps). Such a study can be beneficial to understand security from usability or users' perspective and their involvement in SDLC (in Figure 4.2) for secure app development.

4.5.2 Development Practices for Secure mHealth Apps

Based on the analysis of the developers' responses, we have created a taxonomy of the adopted or recommended practices for different tasks of SDLC that represent guidelines for secure mHealth app development, illustrated in Figure 4.2.

– Lack of interest and awareness in security by users: 62% of our respondents claimed that users are not explicitly interested or aware of security; hence, the developers' compromise security-related requirements in favour of usability and performance. Also, most of mHealth apps stakeholders such as health professionals are non-expert in security to understand the consequences of non-secure apps. Their involvement in SDLC tasks such as requirements engineering and design for secure app development can be seen as a practice that enhances app security and stakeholders' knowledge about security issues.

Needs for future research: Our taxonomy of the developers' recommended practices in Figure 4.2 suggests further investigation on the impact of the identified practices on secure mHealth apps. There is also a need to educate developers and disseminate knowledge about best practices and patterns to improve the development of secure apps.

4.5.3 Motivating Factors to Develop Secure mHealth App

– Consequences of insecure mHealth apps: Developers' perspective (i.e., 85% of respondents in Figure 4.3) suggested that the top factor that motivates secure mHealth app development is to avoid any legal, social, and commercial consequences of deploying insecure apps.

– Vision and reputation of organisation: Developers are also motivated to deliver secure mHealth apps to maintain the vision and reputation of the development organisation they work for, suggested by 81% of the respondents.

– Security team leads to influence secure SDLC: Dedicated team leads or security experts influence app developers to ensure security throughout SDLC. These leaders inspire and guide developers to satisfy security requirements and avoid security risks. However, 36% of the respondents disagreed and suggested that security leaders had not motivated or affected their development process and practices. To further analyse the rationale for their suggestion, we looked into their demographic information (i.e., team size from Figure 2.2) and available data from [45] to know that 50% of those respondents work part-time in a team that consists of eight team members at maximum. This indicates that possibly there is a lack of security leadership within the app development team.

Needs for future research: There is a need for future work to investigate ethical considerations (as a motivating factor) for mHealth apps developers, especially when dealing with stakeholders who are not explicitly interested in or aware of security. Such an examination would explore the role of developers with social and legal responsibilities of secure apps development. Further work can be done to explore the role of security leaders in ensuring security, and how they affect and motivate other team members.

4.6 Conclusions

Mobile computing empowers healthcare stakeholders – offering portable, context-sensitive, and pervasive computing – to produce and consume healthcare services [18]. Mobile apps in general and mHealth apps in particular face critical challenges related to the security and privacy of users' information and health critical data. We conducted an empirical study by collecting, analysing, synthesizing, and documenting responses about secure app development from 97 mHealth app developers from across the world. The study is primarily focused on three objectives expressed as RQs, i.e., (i) what are the challenges? (ii) which development practices are critical? and (iii) how motivating factors impact the development of secure mHealth apps. The results of this study can benefit researchers and practitioners with empirical knowledge about security-specific challenges and opportunities to develop secure mHealth apps.

Chapter 5

End-users' Security Knowledge-Attitude-Behaviour towards mHealth Apps

Related publication:

This chapter is based on MobiQuitous 2020 paper titled "Security Awareness of End-Users of Mobile Health Applications: An Empirical Study" [40].

In the previous chapter, we investigated the security challenges that mHealth apps developers face to develop secure apps, explored the security practices which have been followed by the developers, and identified the motivational factors to ensure the security of mHealth apps. The developers of mHealth apps and the end-users are two actors with distinct but complementary roles to support the secure development and usage of mHealth apps. In Chapter 3 (Section 3.2), we reviewed the security knowledge of end-users towards utilising mHealth apps. This chapter presents an empirical study aimed at exploring the security awareness of end-users of mHealth apps. We utilised the Human Aspects of Information Security Questionnaire (HAIS-Q) that allows measuring security awareness through the Knowledge, Attitude and Behaviour (KAB) model. We collaborated with two mHealth providers in Saudi Arabia to gather data from 101 end-users. The results reveal that despite having the required knowledge, end-users lack appropriate behaviour, i.e., reluctance or lack of understanding to adopt security practices that compromise health-critical data with social, legal, and financial consequences. Our findings provide empirical evidence and a set of guidelines about the security awareness of mHealth apps. This chapter addresses RQ6: What is the level of security knowledge, attitude and behaviour of mHealth apps end-users about using mHealth apps? (Section 5.4.1), and RQ7: What are the relationships between security knowledge, attitude and behaviour? And how do they influence the end-users of mHealth apps? (Section 5.4.2) as highlighted in Table 1.1.

5.1 Introduction

Mobile systems support portable computing that enable users to exploit context-sensitive services such as social networking, crowd-sensing, mobile commerce, and healthcare [85]. Mobile healthcare (i.e., mHealth) relies on (i) embedded sensors of a device (hardware to sense health-critical data), (ii) mobile apps (software to manipulate sensed data), and (iii) networking technologies (protocols to wirelessly transmit data). World Health Organisation (WHO) refers to mHealth as medical healthcare practices, enabled via pervasive technologies, to facilitate stakeholders (e.g., health units, medics, patients) that provide or utilise healthcare services in an automated, efficient, and reliable manner [12]. A widespread adoption of mobile computing has resulted in a rapid proliferation of mHealth apps that range from general apps for decision support and reproductive health to fitness monitoring, activity tracking and nutrition management [5]. The usage of mHealth apps by healthcare practitioners and patients is on a rise with 350,000 such apps available in two of the major app repositories provided by Android and iOS platforms [11]. Research2Guidance (R2G), a consultancy organisation for mHealth technologies, reports that 78,000 new mHealth apps were added to apps stores in 2017 [135] with market revenue for digital health expected to reach USD 31 billion by 2020 [14]. Despite the offered benefits [13] and expected revenues [14] of mHealth systems, security of health-critical data remains a challenge for sustained growth and mass-scale adoption of mHealth apps [1, 8, 15, 16]. The interest of attackers in health-critical data (pulse rate, blood pressure, disease symptoms, etc.) has increased due to its value in the 'black market' as well as social, legal, and financial consequences of compromised data [19]. According to the Ponemon Institute, the price per single medical record escalated from $369 in 2016 to $380 in 2017 due to the regulations and their implementations for health data security [20].

Security of mHealth apps is a critical challenge due to the pervasive environment in which mobile devices continuously ingest health-critical data from embedded sensors, process and persist data inside the device, and transmit it across ad-hoc networks [1, 36]. Experts believe that technical solutions such as authentication and multi-step authorisation cannot address security issues alone, instead, the role of end-users and their understanding of security-related issues is essential to ensure secure mobile computing [37]. Some recent studies have highlighted that social engineering method can be used by hackers to deceive end-users into leaking their private information [4, 38]. Such security lapses are common in mHealth solutions as the end-users usually lack sufficient awareness about security configurations, critical warnings, and consequences of security breaches [39]. A recently conducted study on secure mHealth app development has highlighted that developers who follow a predefined software development lifecycle (SDLC) often assume that they have already delivered a secure app [34]. However, end-users may find security features hard to understand, get deceived by hackers, or be misled by app permissions to disclose private and sensitive information [4]. Due to different categories of mHealth apps (e.g., clinical health, fitness monitoring, and health diagnostics) end-users behave differently depending on the type of apps being used and their security awareness [24, 53]. The existing research on this topic, such as [1, 8, 15], indicate that the security of mHealth apps lags behind the capabilities of hackers that target mHealth apps. In a recent study [34], the authors present developers' perspectives on the challenges, recommended practices, and motivators for developing secure mHealth apps. To date, there has been no empirical effort aimed at investigating the security awareness of end-users regarding the usage of mHealth apps for clinical settings. The study presented in this paper complements the existing research on developers' perspectives [34] by empirically investigating end-users' security awareness of mHealth apps that contain health-critical and other personal data.

We conducted an empirical study - collaborating with two commercial mHealth providers[6] in Saudi Arabia - to survey 101 end-users of mHealth apps for investigating the level of security awareness among app users. Security awareness of end-users refers to the 'required human knowledge, attitude, and behaviour to understand the potential security risks, their implications, and available countermeasures for securing mHealth data' [136]. The surveyed users included patients, clinical practitioners, medical doctors, nurses, and healthcare supervisors affiliated with above mentioned health providers. Demography analysis of the end-users highlight their diverse educational backgrounds, IT skills, years of experience with usage of various mHealth apps on different mobile devices compatible with major mobile computing platforms including Android and iOS. For this study, we utilised the Human Aspects of Information Security Questionnaire (HAIS-Q) [39] that allows measuring security awareness through the Knowledge, Attitude and Behaviour (KAB) model [51]. KAB model refers to a representative study of a specific population that collects information about what is known, believed, and done about a particular topic. Knowledge refers to the level of security understanding by the users, an attitude refers to how the users feel about their knowledge, and behaviour refers to the actions that users may perform to ensure security [39]. To measure and understand the security-awareness, we formulated the following Research Questions (RQs):

RQ6: *What is the level of security knowledge, attitude, and behaviour of end-users about mHealth apps?*

RQ7: *What are the relationships between security knowledge, attitude and behaviour? And how do they influence the end-users while utilising mHealth apps?*

To analyse the collected data for answering the RQs, we used statistical methods, including descriptive analysis, data correlation of survey statements, and regression testing of the recorded responses. The results highlight that end-users' security knowledge strongly influences their attitude (i.e., they

[6] King Fahad Medical City (KFMC) https://www.kfmc.med.sa/EN/Pages/Home.aspx
mHealth app: *iKFMCApp:* https://play.google.com/store/apps/details?id=sa.med.kfmc&hl=en
Dr. Sulaiman Al Habib Medical Group (HMG) https://hmg.com/en/pages/home.aspx
mHealth app: Dr. Sulaiman Alhabib App: https://apps.apple.com/ae/app/dr-sulaiman-alhabib/id733503978

understand what potential threats are). However, end-users' security knowledge has no significant impact on their behaviour (i.e., they lack necessary actions about how to protect data from potential threats). Security training, recommended practices, and adoption of appropriate mHealth apps, both at individual and organisation level are the keys to secure utilisation of mHealth services.

The study provides empirical evidence about the level of end-users' security awareness, i.e., (i) knowledge about recurring security threats, (ii) attitude to securing their data, and (iii) behaviour to mitigate the threats by adopting security practices. This study provides empirical evidence and a set of guidelines to facilitate researchers, practitioners, and stakeholders to develop and adopt secure mHealth apps for clinical practices and public health.

5.2 Related Work

We now review the related work generally classified as (i) security awareness of end-users (Section 5.2.1), and (ii) approaches to measure security awareness (Section 5.2.2). The review helps us to motivate the needs for this study and introduces terminologies and concepts that are used throughout the paper.

5.2.1 Security Awareness of End-Users of mHealth Apps

mHealth apps to support clinical practices are primarily for commercial purposes to enrich users' experience by offering customized functionality and automating trivial tasks of healthcare [36]. Clinical apps collect, process, and transmit more diverse data than general-purpose apps such as fitness monitors and nutrition managers [5]. Data managed by clinical apps include but is not limited to disease symptoms, medical images, prescriptions, insurance policies, and appointments. Currently, healthcare providers are adopting such mHealth apps to empower patients by providing healthcare services that are pervasive, readily available, efficient, and cost-effective [4, 36]. For example, many healthcare services such as diagnosing cardio rates, measuring blood pressure, or detecting fever can be performed on users' end to eliminate prior appointments or personal visits to health units. Moreover, mHealth apps enable end-users to electronically view, share, and manage their medical history [137]. Despite the offered benefits, patients' health-critical data is at risk either due to security flaws in an app [1, 8, 15] or lack of security awareness by app users [4, 15].

Lack of security awareness: A study reported in [24] engaged 24 focus groups with more than 250 participants to examine end-users' attitudes and perceptions regarding mHealth systems being used at healthcare centres. The study revealed that end-users' attitudes were highly contextualized towards security depending on the type of information being communicated, rational for such communication, and consumers of shared information. From the app development perspective, the security of mHealth apps can be enhanced by implementing different control mechanisms (e.g., encryption, authentication, secure storage, access control) that support confidentiality and integrity of data [31]. The adoption of mHealth apps by health providers as well as end-users is on a steady rise, however; some recent studies have reported that low knowledge of security features for end-users is still an issue [4, 15, 113, 114]. The authors in [22] pointed out that today's smartphones implement many security features that range from device lock mechanisms to remote data wiping or end to end encryption. However, even the most advanced systems or sophisticated features of security cannot guarantee users' behaviour and actions that enhance or compromise security and privacy of their classified data [23, 24]. A recent study of more than 450 smartphone owners indicates that they do not use or are unaware of security features provided by default [23]. In the case of mHealth systems, patients as end-users might grant more permissions than necessary, unintentionally share their health data or allow other apps to unnecessarily accessing it [4]. A recently conducted mapping study [30] also indicates that, despite implementing the state-of-the-art security features for mHealth app, lack of knowledge about the security features or privacy permissions by end-users can compromise personal information and health-critical data. The mapping study reviews 365 studies and suggests that security and privacy specific education and training of app developers and users are two of the most critical factors to support secure development and usage of mHealth systems.

Enabling security awareness: Developers, providers, and consumers (commercial enterprises) need to play their roles in increasing the end-users' security awareness [4, 114]. For example, commercial enterprises as consumers of mHealth systems can provide training and guidelines to explain security features of an app to end-users (e.g., doctors, nurses, clinical technicians, patients). Similarly, developers of mHealth apps can engineer their apps to support effective security decisions and facilitate (or enforce) end-users to follow security practices. A typical example of security enforcement by an app can be password management schemes that refuse to accept a weak password or multi-step authentication to access private data [12]. To enhance security awareness, mHealth apps can explicitly indicate access permissions that are essential or optional for end-user to select. As opposed to the adaptive security [138] that enables apps and devices to configure their security protocols at runtime, human-centric security focuses on secure development and usage practices (i.e., users' actions) to enhance the security of mobile systems [34, 39].

5.2.2 Approaches to Measure End-Users' Security Awareness

Security awareness is mostly measured by end-users feedback via surveys or questionnaire-based studies such as [39, 139]. The authors of [54] conducted simulation exercises as controlled experiments to understand participants' behaviour and reactions corresponding to their security awareness about potential threats. Survey or simulation-based approaches to measure security awareness can be helpful to identify users' perspectives and behaviours, highlighting human intellect, attitude, and weaknesses while facing potential security threats [54, 139].

Models for measuring security-awareness: HAIS-Q is a well-known approach that has been used and validated in several studies [39, 51] to measure information security awareness for a diverse group of users (e.g., students, professionals, and volunteers). Some studies have followed the HAIS-Q guidelines [50] to measure the security awareness of smartphone users [140]. The Knowledge, Attitude, and Behaviour (KAB) model that underpins HAIS-Q aims to investigate psychological aspects and their impact on information security awareness [50].

The existing studies, e.g. [24, 53], focus on users' security perceptions of fitness monitoring apps such as activity tracking, and cardio rate analysis. Unlike the fitness monitoring apps, clinical mHealth apps such as patient management systems handle highly sensitive health-critical data and personal information. The scope of this study is to investigate security awareness for the class of clinical health systems in the context of mHealth. From an operational perspective, clinical health apps collect patients' health data, personal information, and medical history that is electronically shared across health care units among different medical professionals – involving a multitude of security issues. To the best of our knowledge, there is no empirical study to investigate end-users' perspectives and security awareness toward using clinical mHealth apps.

5.3 Research Method

In this chapter, we used a survey questionnaire, which indicated in Chapter 2, Section 2.3. The findings of this chapter are based on surveying 101 end-users for mHealth apps. To provide further details, we discuss the research method that comprises four phases, that has been used in this chapter. The overall research method and its individual phases are illustrated in Figure 5.1.

5.3.1 Phase 1 – Design the Study Protocol

We developed the study's protocol in the initial phase, shown in Figure 5.1, that comprises three steps, including (i) specification of research questions (ii) designing survey questionnaire, and (iii) identifying data access methods. As part of this phase, we performed the literature review (Section 5.2) to devise two RQs (Section 5.1). The RQs (i.e., ***RQ7***, ***RQ8***) guided the design of the survey, which was based on the KAB model [50] that underpins HAIS-Q [39, 51].

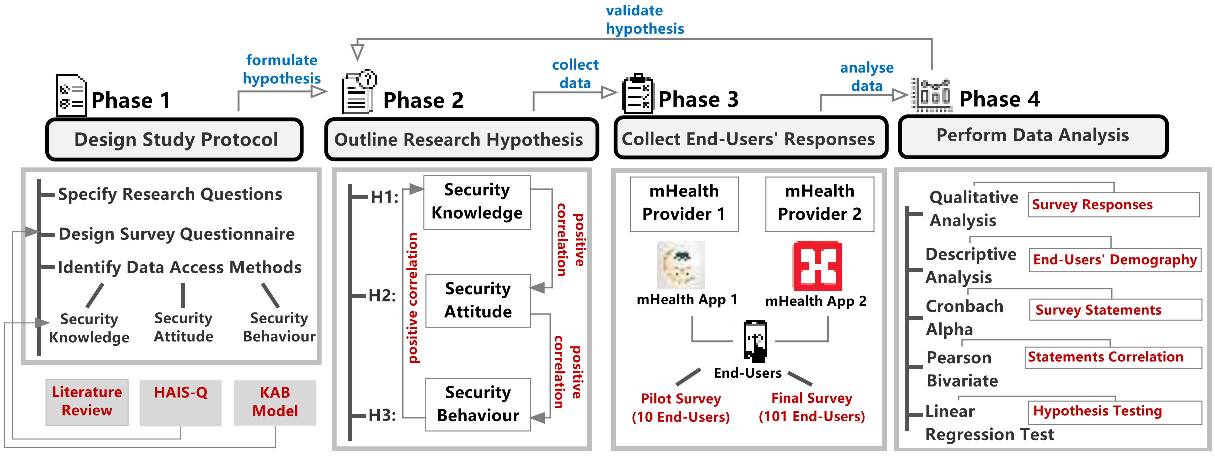


Figure 5.1 An Overview of the Research Method through Utilising KAB Model

Reviewing the literature enabled us to point out the human aspects of mHealth apps. We found that end-users are concerned about four issues (a) *what* methods are used to access their health-critical data, (b) *who* can access their data, (c) for *what* purposes their data is being accessed, and (d) for *how* their data is being stored and transmitted. Figure 5.2 shows four security mechanisms (i.e., solutions) that can be classified as eight security-critical scenarios (i.e., instance of a solution). Following KAB model guidelines [39], we formulated a security knowledge statement, an attitude statement and a behaviour statement for each security-critical scenario as in Figure 5.2. For example, as per Figure 5.2, a knowledge statement can be expressed as *'I should use strong password (not easy to guess) for mHealth app'*. A total of 23 statements (S1 – S23) were formulated that are classified as eight statements for measuring security knowledge, eight statements to measure end-users' attitudes, and seven statements for measuring end-users' behaviour toward using mHealth apps. We provided three options in our survey questionnaire (i.e., True, False, and Don't know) to the end-users. Frequent change or update of the password as a security measure attracts divided views from different security experts [141, 142]. Some experts argue in favour of frequent password updates to make it attack resistant. Others suggest minor updates in password characters or their sequencing (e.g., 'testing123' to 'Testing_123') could reveal a trail of historical passwords - maintained by systems to ensure that a new password is chosen different from old ones - prone to sniffing. The National Institute of Standards and Technology (NIST) guidelines advice that password should be changed in case it got compromised [143], we decided to include frequent password change as a security ensuring technique to investigate end-users awareness towards security risks in the form of password leakage or sniffing. It should be noted that we excluded a statement about data encryption from the behaviour since encrypting data is an automated process of an app and does not represent an actionable task for end-users. Whereas, it is highly recommended that accessing health data must be user-centric, unless there are explicit requirements for data access by third-party apps or systems [12]. End-users should be able to allow or restrict access to their health data at any point of app usage. Figure 5.2 provides an example of how we measured the security awareness of mHealth apps end-users using the KAB model [144].

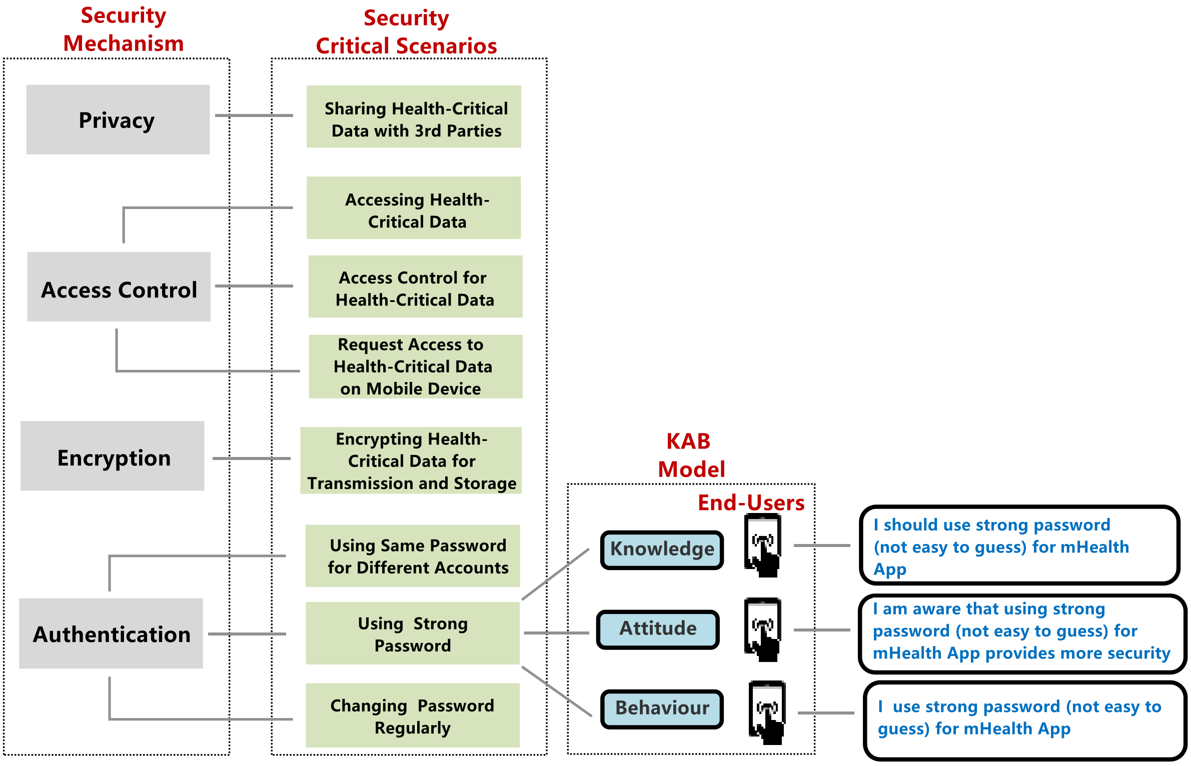

Security Mechanism
Security Critical Scenarios
Privacy
Access Control
Encryption
Authentication
Sharing Health-Critical Data with 3rd Parties
Accessing Health-Critical Data
Access Control for Health-Critical Data
Request Access to Health-Critical Data on Mobile Device
Encrypting Health-Critical Data for Transmission and Storage
Using Same Password for Different Accounts
Using Strong Password
Changing Password Regularly
KAB Model
End-Users
Knowledge
Attitude
Behaviour
I should use strong password (not easy to guess) for mHealth App
I am aware that using strong password (not easy to guess) for mHealth App provides more security
I use strong password (not easy to guess) for mHealth App

Figure 5.2 An Overview of Security Awareness Measurement for End-Users Using the KAB Model

5.3.2 Phase 2 – Outline Research Hypothesis

We outlined three research hypotheses and correlations between them to validate the survey findings as in Figure 5.1 (Phase 2). The research in [51] confirms that raising the knowledge level of information security and procedures would increase end-users' attitude towards information security policy and procedures, which should translate into more risk-averse information security behaviour. Based on the guidelines from [51], we outlined the following hypotheses (**H1** to **H3**):

H1: Security knowledge of the end-users of mHealth apps has a positive correlation with their attitude.

H2: Attitude of the end-users of mHealth apps is positively correlated with their behaviour.

H3: Security knowledge for the end-users of mHealth apps has a positive correlation with their behaviour.

The hypotheses positively correlate end-users' security knowledge, attitude, and behaviour to measure their security awareness for mHealth apps. The hypotheses can be tested based on qualitative analysis of the survey data from end-users of mHealth apps that are detailed next.

5.3.3 Phase 3 – Collect End-Users' Responses

The third phase (i.e., collecting end-users' responses) was explained in detail in Chapter 2, Section 2.3.2.

5.3.4 Phase 4 – Perform Data Analysis

We used a well-known data analysis software, SPSS version 27 (IBM), for the quantitative analysis of our collected data. **Descriptive analysis**, along with mean and Standard Deviation (SD) were performed to report the respondents' demographic data (Figure 2.4) and the survey responses (Figure 5.1, Phase 3). We calculated the **Cronbach Alpha** to measure the reliability and internal consistency of our survey statements. To test the research hypotheses (Figure 5.1, Phase 3), we performed two **Linear Regression** tests, firstly, to predict the respondents' attitudes according to their mean knowledge, and secondly, to predict the respondents' behaviour based on their mean knowledge and mean attitude. To ensure the suitability of such an analysis, the correlation of knowledge, attitude and behaviour was checked. The scatter plot showed that the correlation is linear which allow us to conduct further testing.

5.4 Findings

We now present the results that reflect end-users' security awareness towards the usage of mHealth apps. The results provide answers to ***RQ6*** in Section 5.4.1, and ***RQ7*** in Section 5.4.2.

5.4.1 End-Users' Security Knowledge, Attitude, and Behaviour (RQ6)

As per the research methodology (Phase 4, Figure 5.1), we applied a number of statistical methods to formalize data analysis (measuring consistency, correlation, and description) of end-users' responses presented in Table 5.1 - Table 5.5, detailed in [144].

5.4.1.1 Measuring Consistency of Survey Statements

To answer ***RQ6***, Table 5.1 below presents Cronbach's alpha to measure the internal consistency of the survey statements, i.e., how our survey statements are closely related to measure end-user security knowledge, attitude, and behaviour while using mHealth apps [61]. Cronbach's alpha helped us to determine the reliability of the measurement values (end-users' responses that are captured using multiple Likert questions). Table 5.1 highlights that three constructs each having a specific value (i) security knowledge = 0.820, (ii) attitude (towards security) = 0.732, and (iii) behaviour (while using mHealth app) = 0.722. The values of Cronbach's alpha were obtained by calculating the results of each dimension (e.g., only the attitude related to the statements were calculated together). Our results indicate that we met the minimum acceptable coefficient value (i.e., ≥ 0.7).

Table 5.1 Cronbach's Alpha for End-Users' Knowledge, Attitude, and Behaviour.

Constructs	Cronbach's alpha
Knowledge	0.820
Attitude	0.732
Behaviour	0.722

5.4.1.2 Measuring Correlation between Survey Statements

We conducted **Pearson product-moment correlation** (Pearson's correlation) [145] to test the correlation (i.e., strength and direction of association) between the survey statements for obtained data, presented in Table 5.2 –Table 5.4. Specifically, Table 5.2 –Table 5.4 show the correlation strength and significance among the survey statements for each dimension of security awareness (i.e., knowledge, attitude, and behaviour). All our survey statements showed a positive relationship ranging from strong (i.e., 0.86: *access to health data*) to a very weak (i.e., 0.02: *changing the password regularly*) relationship, as in Table 5.2. Only two statements in the attitude dimension (i.e., *encrypting health data during transmission and storage*, and *changing the password regularly*) showed a very weak negative relationship, as in Table 5.3. On the other hand, our test results imply that 61% of our survey statements had a significant relationship (i.e., 48% at the 0.01 level, and 13% at the 0.05 level). This means that about 39% of our survey statements showed that there was no significant relationship between end-users security knowledge, attitude, and behaviour. For those reasons which are related to the correlation strength and their significance, we ensured that our survey items are measuring the interest through reviewing and clarifying any ambiguity.

Table 5.2 Correlation for Security Knowledge Statements

Security Implementation Strategies	1	2	3	4	5	6	7	8
1. Anonymizing health-critical data with third parties.	1							
2. Accessing health-critical data.	.86**	1						
3. Controlling access to health-critical data.	.64**	.64**	1					
4. Request access to health-critical data on mobile device.	.67**	.56**	.44**	1				
5. Encrypting health-critical data during transmission and storage.	.47**	.54**	.35**	.50**	1			
6. Using same password for different accounts.	.27**	.31**	.18	.16	.16	1		
7. Using a strong password.	.27**	.33**	.35**	.20*	.17	.71**	1	
8. Changing the password regularly.	.24**	.19	.17	.31**	.02	.15	.33**	1

Table 5.3 Correlation for Attitude Statements

Security Implementation Strategies	1	2	3	4	5	6	7	8
1. Anonymizing health-critical data with third parties.	1							
2. Accessing health-critical data.	.57**	1						
3. Controlling access to health-critical data.	.53**	.53**	1					
4. Request access to health-critical data on mobile device.	.51**	.37**	.45**	1				
5. Encrypting health-critical data during transmission and storage.	.35**	.24*	.21*	.32**	1			
6. Using same password for different accounts.	.18	.05	.25*	.22*	.18	1		
7. Using a strong password.	.08	.17	.25*	.02	.06	.42**	1	
8. Changing the password regularly.	.04	.19	.11	.21*	-.05	.14	.42**	1

Table 5.4 Correlation for Behaviour Statements

Security Implementation Strategies	1	2	3	4	5	6	7
1. Anonymizing health-critical data with third parties.	1						
2. Accessing health-critical data.	.66**	1					
3. Controlling access to health-critical data.	.52**	.58**	1				
4. Request access to health-critical data on mobile device.	.48**	.42**	.49**	1			
5. Using same password for different accounts.	.18*	.22*	.09	.06	1		
6. Using a strong password.	.15	.18	.17	.17	.41**	1	
7. Changing the password regularly.	.13	.20*	.04	.18	.18	.26**	1

**. Correlation is significant at the 0.01 level (2-tailed). *. Correlation is significant at the 0.05 level (2-tailed).

5.4.1.3 Descriptive Analysis of Responses

Table 5.5 presents a descriptive summary of end-users' responses (**R1 – R101**) for statements (**S1 – S23**) in our survey [144]. For quantification and simplification of data analysis, we assigned numbers to the given options (i.e., True=1, Don't know=2, False=3). Frequency, percentage, mean and SD are presented in Table **5.5**. Since the middle value is 2, a mean of less than 2 implies that the respondents have agreed to the statement (True = 1). Whereas, a mean of greater than 2 implies that respondents have disagreed with the statement (False = 3). Our findings indicate that end-users have different opinions about (i) *what* they need to know (i.e., knowledge), (ii) *why* they should know (i.e., attitude) and (iii) *how* they should behave (i.e., behaviour) when it comes to using mHealth apps. For example, end-to-end data encryption (e.g., using Transport Layer Security (TLS) with 128-bit encryption) is a method to secure data that travels across devices, over various networks, and accessed by a third-party. To compare the variance, we provided two encryption related-statements (i.e., S5 and S13) to examine our respondents' knowledge and attitude toward applying encryption within the used mHealth apps. Only 43/101 (i.e., 42.6%) of end-users believed that they should know whether or not their health data, which have been collected by mHealth apps, is sent and stored in an encrypted format. Whereas, 47/101 (i.e., 46.5%) of our respondents indicated that they are not aware whether or not their health data, which have been collected by mHealth apps, are encrypted during transmission and storage. In fact, one respondent [**R33**] commented that *"[…] the responsibility to protect data is one of the patient's rights to be fulfilled by health service provider"*. Thus, there is a need at app providers' end to share information with end-users about the existing features which make the apps more secure and trustable.

Our results indicate that the respondents' level of security knowledge, attitude, and behaviour towards using mHealth app vary. Such variations are primarily due to a number of factors that are presented in the demographic details of the end-users (Figure 2.4). This indicates that respondents were not confident about some of the existing security measures implemented in the mHealth apps. The results indicate security-specific documentation or education should be delivered to end-users from mHealth app providers.

Table 5.5 Descriptive Summary of Responses to the Statements in the Survey (Sample Size: N=101)

Survey Statements	True (1), n (%)	Don't know (2), n (%)	False (3), n (%)	Mean (SD)
Knowledge related statements				
S1: I should be informed when my health data, which have been collected by mHealth apps, are being shared with third parties, such as other hospitals or clinics.	68 (67.3)	17 (16.8)	16 (15.8)	1.49 (.756)
S2: I should know who accesses my health data and for what purpose.	61 (60.4)	25 (24.8)	15 (14.9)	1.54 (.742)
S3: I should have control of my health data.	54 (53.5)	25 (24.8)	22 (21.8)	1.68 (.812)
S4: I should know that some apps request access to my health data (e.g., marketing purposes).	50 (49.5)	35 (34.7)	16 (15.8)	1.66 (.739)
S5: I should know whether my health data, which have been collected by mHealth apps, is sent and stored in an encrypted format.	43 (42.6)	38 (37.6)	20 (19.8)	1.77 (.760)
S6: I should use different passwords for different accounts and apps.	72 (71.3)	16 (15.8)	13 (12.9)	1.42 (.711)
S7: I should use a strong password (not easy to guess) for the mHealth app.	79 (78.2)	14 (13.9)	8 (7.9)	1.30 (.609)
S8: I should change the password for the app regularly.	60 (59.4)	23 (22.8)	18 (17.8)	1.58 (.778)
Attitude related statements				
S9: I am aware that my health data, which have been collected by mHealth apps, will not be shared with third parties, such as other hospitals or clinics.	56 (55.4)	23 (22.8)	22 (21.8)	1.66 (.816)
S10: I am aware of who accesses my health data and for what purpose.	37 (36.6)	36 (35.6)	28 (27.7)	1.91 (.801)
S11: I am aware that having control of my health data provides security.	51 (50.5)	25 (24.8)	25 (24.8)	1.74 (.833)
S12: I am aware that some apps request accessing health data more than they need.	44 (43.6)	37 (36.6)	20 (19.8)	1.76 (.764)
S13: I am aware that my health data, which have been collected by mHealth apps, are encrypted during transmission and storing.	32 (31.7)	47 (46.5)	22 (21.8)	1.90 (.728)
S14: I am aware that using one password for different accounts and apps will make it easy for me; but, it is insecure.	71 (70.3)	15 (14.9)	15 (14.9)	1.45 (.741)
S15: I am aware that using a strong password, that's not easy to guess, for mHealth app provides security.	82 (81.2)	8 (7.9)	11 (10.9)	1.30 (.656)
S16: I am aware that changing the password for the app regularly provides security.	62 (61.4)	17 (16.8)	22 (21.8)	1.60 (.826)
Behaviour related statements				
S17: I get informed when my health data, which have been collected by mHealth apps, are being shared with third parties.	49 (48.5)	23 (22.8)	29 (28.7)	1.80 (.860)
S18: I know who access my health data and for what purpose.	38 (37.6)	30 (29.7)	33 (32.7)	1.95 (.841)
S19: I already have control of my health data.	47 (46.5)	24 (23.8)	30 (29.7)	1.83 (.861)
S20: I may accept or deny the request based on what I think is secure.	45 (44.6)	29 (28.7)	27 (26.7)	1.82 (.829)
S21: I use different passwords for different accounts and apps.	64 (63.4)	12 (11.9)	25 (24.8)	1.61 (.860)
S22: I use a strong password, that's not easy to guess for mHealth app.	83 (82.2)	5 (5.0)	13 (12.9)	1.31 (.689)
S23: I change my password of the app regularly.	45 (44.6)	9 (8.9)	47 (46.5)	2.02 (.959)

5.4.2 Correlation between End-Users Security Knowledge, Attitude, and Behaviour (RQ7)

To answer ***RQ7***, i.e., measuring the correlation, we utilised the KAB model (Figure 5.2) that measures end-user security awareness by examining three dimensions to test the outlined hypotheses (H1 – H3). Therefore, we tested the hypothesis that there is a significant positive correlation between (a) the respondents' knowledge which affects their attitude, and (b) the respondents' knowledge and attitude, which affect their behaviour. We assigned the predictor variables to give us an estimation of the significance, and for that, we conducted regression analysis using SPSS software. As per the KAB model [39, 51] to measure the correlation, we considered knowledge as an exogenous variable and considered attitude and behaviour as two endogenous variables [51]. Thus, we performed two linear regression tests (i.e., one simple regression and one multiple regression), both detailed below, to assess the correlation of our variables.

5.4.2.1 Simple Regression Test - Predicting Attitude based on Knowledge

A simple regression test is aimed to see whether we could predict attitude based on the knowledge that end-users had or not. Figure 5.3 presents our findings based on the correlation among knowledge, attitude and behaviour. Our analysis revealed that the knowledge variable had a statistically significant impact on the attitude variable producing R^2_1= 0.602, (B=0.718, t= 12.236, $p < .001$). This means that our respondents' knowledge accounted for 60.2% of the variance in their attitude, which implies that, respondents' knowledge is positively related to their attitude. For example, the survey statements (S14: '*I am aware that using one password for different accounts and apps will make it easy for me; but, it is insecure*') was endorsed (True = 1) by 70% of the end-users. Similarly, 70% of the end-users agreed (S6: '*I should use different passwords for different accounts and apps*'). This correlation equated to B= 0.718 for H1: Security knowledge for the end-users of mHealth apps has a positive correlation with their attitude.

5.4.2.2 Multiple Regression Test - Predicting Behaviour based on Knowledge and Attitude

The second regression tests the possibility of predicting end-users' behaviour based on knowledge and attitude. Our analysis also revealed that both knowledge and attitude have a statistically significant impact on behaviour producing R^2_2= 0.526, as Figure 5.3. The results of the multiple regression test indicate that our respondents' knowledge and attitude account for 52.6% of the variance in their behaviour. Although, coefficient results indicate that attitude predictor is statistically significant, (B = .716, t = 5.713, $p < .001$), yet, knowledge predictor is not statistically significant, (B = .125, t = 1.076, $p < .285$). For example, we notice that many respondents, such as **R32**, **R34**, **R42**, **R45**, agreed that they knew and believe (i.e., knowledge and attitude) that mobile apps would be secure when using different passwords for different accounts and apps. However, their actual behaviour is not representing their knowledge and attitude. By reviewing the obtained data, particularly knowledge and behaviour responses, we noticed a contradiction between what respondents should know (i.e., their knowledge) and how they should behave (i.e., their behaviour). For instance,

- *Knowledge and Attitude:* 59% of our respondents reported that they knew that changing the password for the app frequently (S8 in Table 5.5) would enhance security.
- *Knowledge and Behaviour:* In reality, 47% of our respondents indicated that they did not change the password frequently, and thus, behaving according to the knowledge which they already had.

The results of the multiple regression test support (B = .716, $p < .001$) for H2: Attitude of the end-users of mHealth apps is positively correlated with their behaviour and reject (B = .125, $p < .285$) H3: Security knowledge for the end-users of mHealth apps has a positive correlation with their behaviour. Overall, our results can be more robust in case we could have involved more respondents (e.g., sample size N = 300). We believe that the outcomes support the used model, and it is acceptable to evaluate the end-users' security awareness toward using mHealth apps. The findings indicate that some of the respondents had good knowledge and attitude but did not demonstrate good behaviour, which could expose them to a significant risk. This is a clear indication of the need of providing end-users with suitable training to promote good security behaviour. Such a strategy would also help to enhance their awareness when using mHealth apps.

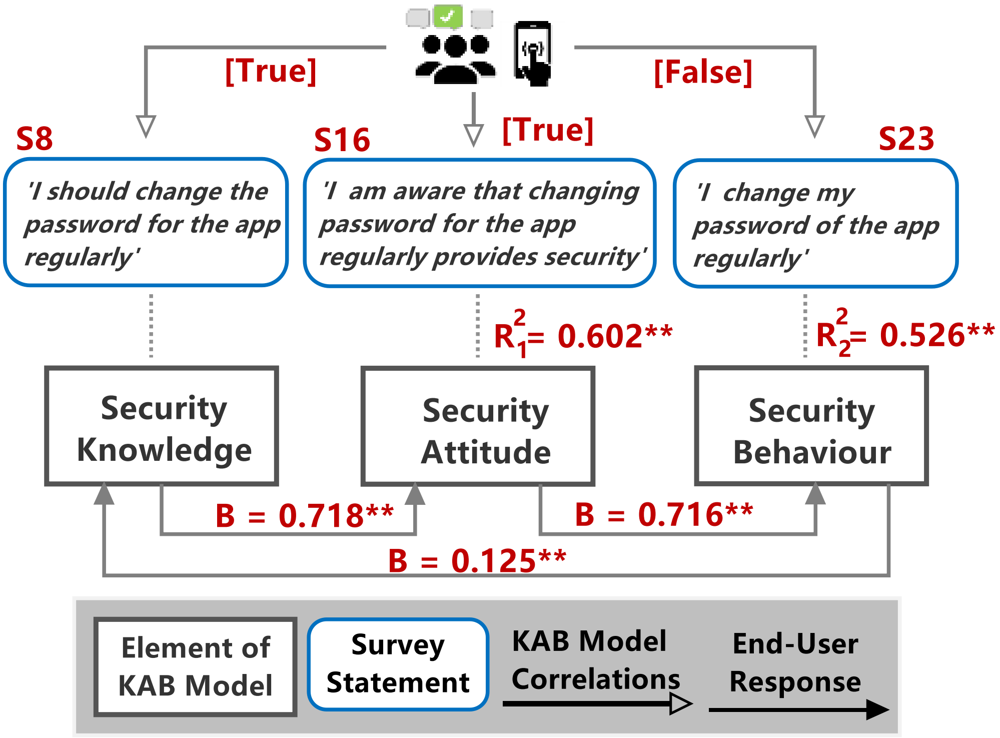


Figure 5.3 Results in support of the KAB component of the HAIS-Q model

5.5 Discussion

We now discuss the key results of our study and highlight the potential future work to extend this study's findings.

5.5.1 Overall Security Awareness of End-Users

The answer to ***RQ6*** indicates end-users' security awareness for mHealth apps varies depending on different factors such as educational backgrounds, prior experience, IT specific understanding and age groups (Figure 2.4). The analysis of the data in Table 5.3 and linking it with demographic information in Figure 2.4 indicates that end-users' of *age group* 30 – 49, who have *moderate or advanced knowledge of IT* systems and have at least a *bachelor's degree* are well aware of the security issues pertaining to their health-critical data and personal information. However, the security knowledge of end-users does not always translate to the required behaviour that can make their data more secure. For example, despite the awareness about the security criticality of health data, end-users rarely choose complex passwords and feel it inconvenient to frequently change passwords. By combining demographic details and statistical data analysis, we imply that the level of security awareness varies and it is primarily influenced by users' behaviour that can make their data more or less secure. ***RQ7*** aims to investigate a human-centric view towards security-aware usage of mHealth apps with a focus on (i) what the end-users' know (i.e., knowledge), (ii) how they perceive security threats based on their knowledge (i.e., attitude), and (iii) why they should act to enable or enhance security (i.e., behaviour). This RQ does not answer what steps can be taken to enhance users' knowledge, change their attitudes, and motivate them to behave in a manner that ensures the security and privacy of health-critical data.

Needs for future research: It is interesting to observe that many respondents do not act according to their knowledge and attitude as shown in Table 5.2 - Table 5.3. This can be due to many factors such as the need for manual actions to enhance security (e.g., frequent password changes) and lack of understanding of the consequences of security breaches. Future research can be focused on the effectiveness of formal training or security education, such as workshops, presentations, or hands-on sessions that enhance the security awareness of mHealth apps end-users. The scope of such research can go beyond mHealth apps to also investigate end-users' KAB towards other mobile apps that deal with sensitive information (e.g., mobile banking, social networking, mobile commerce). However, such an investigation requires customisation of survey statements based on the type of app being used. An investigation of the impact of security training on end-users' security awareness can help to identify best practices, processes, and patterns that can be adopted as guidelines. As part of the future research, we aim to explore the practical approaches for security and their impacts on end-users by means of attack simulation and controlled experimentation to analyse human behaviour.

5.5.2 Correlation between KAB Model for Security Awareness

The study [51] has indicated that better knowledge is associated with better attitude, and both are associated with better behaviour, and that leads to better security awareness about security risks and counter-measures. The findings of ***RQ7*** indicate that our respondents' knowledge has a positive effect on their attitude, suggesting that the respondents have the necessary knowledge and attitude to ensure the security of mHealth apps. However, the analysis indicates that our respondents' knowledge and attitude does not affect their self-reported behaviour (Figure 5.3). The explanation for our findings can be related to organisational factors (e.g., lack of security policy and guidelines) and individual factors (e.g., personality, app usage experience, and security perception). Since our study is more focused on the security *awareness of end-users toward using mHealth apps, the self-reported behaviour* results are slightly different than [51]. We targeted the respondents who are mainly using their own devices, and there are no assigned security policies and guidelines that they should follow. The study [51] investigates how employees adhere to the existing security policy and guidelines when using organisations' computers for network-based applications.

Needs for future research: mHealth apps capture, process, and share health-critical data, and lack of security policy and guidelines for end-users is a critical challenge to be addressed. There is an urgent need for research efforts to develop appropriate security policies and guidelines for using mHealth apps so that end-users understand how to prevent security-related risks while using the apps. Furthermore, the security policy and guidelines would explain the right actions that end-users need to take in different circumstances. At the same time, providing suitable security awareness regarding the policy and guidelines for the end-users is as important as developing secure mHealth apps.

5.6 Conclusion

mHealth apps have started to revolutionize the healthcare sector – empowering stakeholders such as governments, health units, medics, and patients – by offering context-sensitive and pervasive health services. Despite the offered benefits, mHealth apps are prone to security issues related to health-critical data and personal information of app users. We conducted an empirical study by using well established models like KAB and HAIS-Q to measure human aspects of mobile security in the domain of mHealth systems. Specifically, we collected, synthesized, analysed, and documented responses from 101 end-users of two mHealth apps regarding their security awareness towards app usage. The analysis of the demography data of the end-users' highlights that factors such as level of IT knowledge, age group, past experience with mHealth apps, mobile platforms they use, and educational backgrounds influence end users' security awareness (i.e., users' knowledge, attitude, and behaviour). The results suggest that end-users' security-specific:

- Knowledge strongly influence their attitude towards the security of mHealth apps. This means that users are aware of risks (e.g., stealing/tempering of health-critical data) and like to mitigate them (e.g., app support for data encryption).
- Knowledge does not significantly influence their behaviour. This means that users are aware of risks (e.g., private data shared with third parties for targeted ads) but are reluctant or unware of appropriate actions that mitigate risks (e.g., setting privacy preferences to restrict undesired data access).

Chapter 6

End-Users' Knowledge and Perception about Security of Mobile Health Apps

Related publication:

This chapter is based on Journal of Systems and Software paper titled "End-Users' Knowledge and Perception about Security of Mobile Health Apps: A Case Study with Two Saudi Arabian mHealth Providers" [52].

In the previous chapter, we measured the security awareness of end-users when using clinical mHealth apps by utilising the Knowledge, Attitude and Behaviour (KAB) model. In Chapter 3 (Section 3.2), we reviewed the security concerns of end-users towards utilising mHealth apps. This chapter presents an empirical investigation about the security awareness of end-users of mHealth apps. We collaborated with two mobile health providers in Saudi Arabia to survey 101 end-users, investigating their security awareness about (i) existing and desired security features, (ii) security-related issues, and (iii) methods to improve security knowledge. Results indicate that majority of the end-users are aware of the existing security features provided (e.g., restricted app permissions); however, they desire usable security (e.g., biometric authentication) and are concerned about privacy of their health information (e.g., data anonymization). End-users suggested that protocols such as session timeout or two-factor authentication positively impact security but compromise usability. Security awareness via peer guidance, or training from app providers can increase end-users' trust in mHealth apps. The results provide an empirical evidence and a set of guidelines to develop secure and usable mobile health apps. This chapter aims to address RQ8: To what extent are mHealth app end-users aware of the existing security features? And, what are the security features that mHealth app end-users wish to have in mHealth apps in the future? (Section 6.4.2), RQ9: What security issues have been faced by end-users during their usage of the employed security features within mHealth apps? (Section 6.4.3), and RQ10: What methods help end-users to improve their security knowledge regarding mHealth apps? (Section 6.4.4) as highlighted in Table 1.1.

6.1 Introduction

mHealth apps gained remarkable growth by offering advanced solutions that aim to support healthcare interventions based on end-users' conditions [1]. mHealth apps can be used to sense changes in human body measurements (e.g., blood pressure, glucose level, etc.), transmit data to doctors, or even generate alerts relevant to a patient's condition through the app [146]. Despite the promising benefits [13] and generated profits [14], security of health-critical data remains a challenge for the sustainability and mass-scale adoption of mHealth apps [1, 8, 15-18]. End-users' health records (e.g., disease symptoms, blood pressure, clinical reports, etc.) are on the rise due to the value of data in the 'black market' along with socio-legal consequences of the compromised data [19]. A report by Ponemon Institute[7] indicated

[7] Ponemon Institute available at https://www.ponemon.org/

that the average price of each medical record has increased from USD 369 in 2016 to USD 380 in 2017 due to policies, regulations, and their implementations for securing health-critical data [20]. Medical records contain personal data (name, age, gender, address, contact detail etc.) and health-critical information (such as disease, prescriptions, treatment, etc.). This information could be used to embarrass the patients, or could be used to have illegal drugs, receive treatment or make fake medical claims to insurance companies [21]. While mHealth apps can enhance further features to address the security, human-centric knowledge and practices to protect critical information are essential and need to be complemented. A study by Mylonas et al. [22] highlighted that mobile devices implement a multitude of security features including device lock, remote data wipe, and end-to-end encryption. However, even the most sophisticated security features can never guarantee human behaviour (e.g., privacy leakage, unwanted access grant) that enhances or compromises device protection and/or data security [23, 24].

Security and privacy of mHealth apps can be viewed from two different perspectives referred to as the developers' perspective (i.e., security-aware development) and end-users' perspectives (i.e., security-aware usability). Developers' perspective focuses on practising secure SDLC to engineer apps by prioritizing security-specific requirements, implementing data encryption methods and performing vulnerability testing. For example, an empirical study [34] focuses on developers' perspectives about critical challenges, recommended practices, and motivating factors to develop secure mHealth apps. Developers who practice secure SDLCs to engineer mHealth apps often assume that the delivered app is secure, however; end-users of the app in many instances may find security features hard to understand, get deceived by hackers to leak private information, or mislead by app permissions to disclose classified data. A study [24] engaged 24 focus groups having more than 250 participants to investigate the attitudes and perceptions of app users regarding mHealth systems being used at healthcare centres. Existing research indicates that sophisticated cyber-attacks jeopardize mobile apps and implemented security features often become obsolete due to state-of-the-art techniques for data infiltration/exfiltration [1, 8, 15]. To ensure security and ultimately strengthen the confidence of stakeholders in adopting mHealth systems, there is a need to unify both the developers' and end-user's perspectives of security. A mapping study [30] highlights that there is little research on understanding and measuring the security awareness of end-users of mobile and ubiquitous health systems.

To empirically investigate the security awareness of end-users[8] towards using clinical mHealth apps, we conducted a case study survey research by collaborating with two large mHealth providers in Saudi Arabia. In our context, security awareness of end-users refers to '*human-centric perception of (existing and desired) security features, experiences with security issues, and understanding of methods for secure usage of mobile health systems.*' For example, biometric verification of users by an app is perceived as a security feature, excessive or undesired permissions (e.g., reading contacts or voice data) is considered a security issue, while security training (e.g., electronic material or workshops) enables end-users to improve security-awareness. End-users included patients and medical professionals with diverse experiences of clinical practices in varying roles including but not limited to medical doctors, nurses, and healthcare supervisors. Demographic analysis of end-users' data highlighted their educational backgrounds, IT skills, years of experience using mHealth systems compatible with major mobile platforms, including Android and iOS. To objectively measure and understand security awareness, we identified three Research Questions (RQs) to be investigated:

RQ8: *To what extent are mHealth app end-users aware of the existing security features? And, what are the security features that mHealth app end-users wish to have in mHealth apps in the future?*

RQ9: *What security issues have been faced by end-users during their usage of the employed security features within mHealth apps?*

RQ10: *What methods help end-users to improve their security knowledge regarding mHealth apps?*

In order to answer these RQs, we gathered data from 101 respondents through a survey questionnaire and synthesized the survey data, using statistical methods in two different phases. Data analysis included (i) descriptive analysis to investigate end-users' responses and (ii) qualitative analysis to

[8] We use the term *end-users*, *participants*, *respondents* interchangeably throughout the paper, all referring to *users* of mHealth apps that were engaged in this study for their feedback and responses.

identify, analyse, and report frequent overlaps in users' responses, representing patterns of security awareness. The results highlight significant variation in end-users' security awareness and factors such as educational background, level of IT knowledge, and prior experience with mHealth apps reflected positive impacts on security awareness. End-users perceive controlled app permissions, user authentication and security customization as useful existing features and they desire usable security along with privacy preservation as missing but required features of their mHealth apps. Security protocols such as session timeouts, excessive permission requests or multi-stage authentication enhance app security but hinder app usability. A lack of security education and training by mHealth app providers contributes to reluctance to the adoption of mHealth apps. We outline the primary contributions of this research as:

- Reporting an exploratory case study that investigates mHealth users' perceptions, issues and knowledge about security of mHealth apps. The results of our study provide a taxonomy and a benchmark to evaluate the effectiveness of security features offered by mHealth apps.
- An empirically derived set of guidelines to facilitate researchers, practitioners, and stakeholders to develop and adopt secure and usable of mHealth apps for clinical practices and public health.

6.2 Research Method

In this chapter, we used a survey questionnaire, which is detailed in Chapter 2, Section 2.3. The findings of this chapter are based on surveying 101 end-users for mHealth apps.

6.3 Findings

We now present the findings of the study to answer the outlined RQs. Answers to the RQs are presented in the dedicated sections focused on end-users': (i) *security perceptions* (***RQ8***) in Section 6.3.1, (ii) *security issues* (***RQ9***) in Section 6.3.2, and (iii) *security knowledge* (***RQ10***) in Section 6.3.3. Technical details of the statistical analysis and hypotheses testing about security awareness in the context of end-user demography (Figure 2.4) are presented in Section 6.4.2 (Table 6.2 – Table 6.3). For the sake of illustration, Table 6.4, Table 6.5, and Table 6.6 complements the presentation of the study results (***RQ8***, ***RQ9***, and ***RQ10***) by exemplifying end-user responses, denoted as [**Rn**], where n represents a numerical value ranging from 1 to 101 for unique identification of each response. For illustrative reasons, we provide visual markings, wherever required, indicated as 🗨 to express 'User Response' 📜 and to express conclusive summary based on data analysis.

6.3.1 End-users' Understanding of Existing Security Features and the Desired Security Features (RQ8)

In this section, we answer ***RQ8*** which aims to investigate security awareness in terms of understanding of the existing features and the desire for futuristic features that enable or enhance app security. Some recent studies, such as [23], have suggested that users' perception about security is based on their (a) knowledge of the existing features (i.e., available security measures) and (b) understanding of the desired functionality (i.e., required security measures). The questionnaire-based study, which contains open-ended questions, and closed questions, is a suitable method to capture the knowledge of end-users, as in [23]. Therefore, we investigated the security based on users' awareness about existing features using closed questions in Section 6.3.1.1, and recommendations about the desired features that can optimize security measures and strengthen users' trust in the app in Section 6.4.1.3.

6.3.1.1 Security Awareness about Existing Features

To understand security awareness regarding the existing features (**Q10**, per survey design in Figure 2.3, Phase 1), we formulated eight Security Statements referred to as **SA1 – SA8**, visualized in Figure 6.1. The statements were formulated based on identifying eight distinct security features provided in the chosen mHealth apps (iKFMC app, Dr. Sulaiman Alhabib app, from Figure 2.3). The statements were divided into four categories namely (1) App Permissions [**SA1**, **SA2**, **SA3**], (2) User Authentication [**SA4**, **SA5**], (3) User Control [**SA6**, **SA7**], and (4) Feedback and Reporting [**SA8**]. The statements were classified into categories based on their relevance to objectively assess: how end-users perceive security (and privacy) of their health-critical data while using the provided features by mHealth apps. For example, the statement **SA1–SA3** that corresponds to users' consent and permission to share their data was organised under the App Permissions category. Each of the eight statements was presented as a five scale Likert option (i.e., *always*, *sometimes*, *rarely*, *never*, and *don't know*) to determine users' awareness of an existing feature.

Regarding the apps, the existing security features refer to implemented controls, policies, and procedures (e.g., authentication protocols, users' permissions, data wiping) to enable app security. Table 6.3 provides examples of users' responses corresponding to **SA1 – SA8**. An overview of the results is illustrated in Figure 6.1. The uncertainty in users' responses is reflected through their selection of options like *Sometimes* and *Rarely*. We exemplify some responses (**SA3**, **SA7**) to explain App Permissions and User Control features where end-users indicated a lack of security perception as:

'the app sometimes collects data without (my) permission' **[R43]**, and *'the app rarely provides the feature of wiping all health data in case the device is lost or stolen'* **[R4]**.

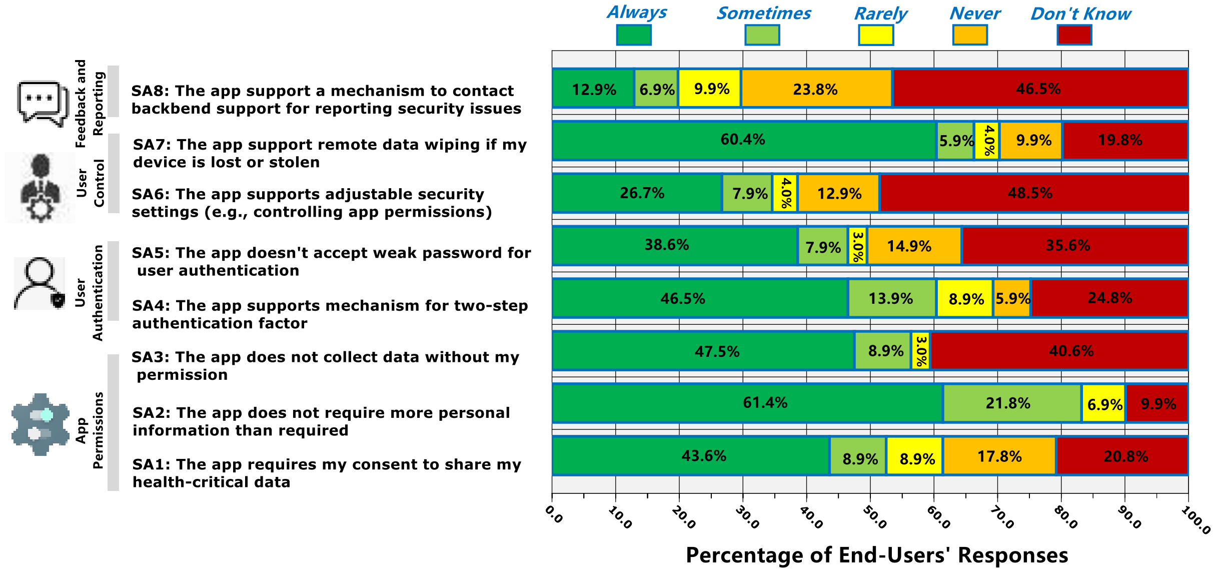


Figure 6.1 End-Users Awareness of Existing Security Features (n=101)

The results indicate that more than 40% of the respondents suggested that they were unaware of app permission to access their private data, whereas only about 20% indicated they lacked knowledge about wiping their health-critical data. It is important to mention that an overwhelming majority, i.e., more than 83% of respondents, suggested that they were aware that apps did not collect more personal information than required (SA2). For example, as in Table 6.3, the response **[R36]** indicated that end-users perceived the app as easy to use for authentication and did not collect excessive information.

Overall, it is believed that end-users still lack awareness about the implemented security features within the apps. For example, 48.5% of our respondents do not know whether the provided apps contain adjustable security settings or not (**SA6**). Also, 46.5% do not know whether the examined apps have the feature of contacting backend support to report security issues (**SA8**). These percentages can be considered very high in representing nearly half of the surveyed respondents. Thus, further support is needed to familiarize end-users with current security features, when and how they could be utilised.

6.3.1.2 Respondents' Security Awareness Based on Demography Information

As indicated in Chapter 2, Section 2.3.3 Phase 3 – Perform Data Analysis, we conducted the Independent-Sample T-test for gender since we were comparing two independent populations (i.e., male and female), and the Kruskall-Wallis H test for more than two independent populations (e.g., IT knowledge level, age group, etc.). These statistical tests helped us to determine whether there were statistically significant differences in the level of security awareness among the defined groups of users.

We further investigated the significant differences for the groups whenever applicable (i.e., whenever p-value < .05). We used the Mann Whitney U test to compare the median differences between the overall extents [54, 55]. For each demographic data, we tested the null hypothesis (i.e., *H0: there is no significant difference*) against the alternative hypothesis (i.e., *H1: there is a significant difference*), whereas *µ1, µ2, …, µk* refers to population means.

Table 6.1 Variables and Corresponding Codes in SPSS for End-User Perspectives Study

Security Awareness	Code	Gender	Code	IT Knowledge Level	Code	Age Group	Code	Formal Education	Code	Frequency of Usage	Code
Never	**1**	*Male*	1	*Little or no knowledge*	**1**	*18 – 29 young adult*	**1**	*High school or less*	**1**	*At least once a day*	**1**
Rarely	**2**									*At least once a week*	**2**
I don't know	**3**			*Moderate knowledge*	**2**	*30 – 49 adult*	**2**	*Diploma*	**2**	*At least once a month*	**3**
		Female	2					*Bachelor degree*	**3**	*At least once every 3 months*	**4**
Sometimes	**4**			*Advanced knowledge*	**3**	*Above 50 senior*	**3**	*Higher diploma*	**4**	*At least once every 6 months*	**5**
Always	**5**							*Master's or PhD*	**5**	*At least once a year*	**6**

Table 6.2 Differences in Security Awareness Based on the Characteristics of Study Respondents

Demography Data Category	Identified groups	N (%)	p-value
Gender	*Male*	61 (59%)	.295
	Female	40 (41%)	
IT Knowledge Level	*Little or no knowledge*	31 (31%)	.006
	Moderate knowledge	49 (48%)	
	Advanced knowledge	21 (21%)	
Age Group	*18 – 29 young adult*	33 (33%)	.141
	30 – 49 adult	60 (59%)	
	Above 50 senior	8 (8%)	
Formal Education	*High school or less*	11 (11%)	.007
	Diploma	13 (13%)	
	Bachelor degree	45 (45%)	
	Higher diploma	10 (10%)	
	Master's or PhD	22 (22%)	
Frequency of Usage	*At least once a day*	6 (6%)	.797
	At least once a week	14 (14%)	
	At least once a month	37 (37%)	
	At least once every 3 months	23 (23%)	
	At least once every 6 months	14 (14%)	
	At least once a year	7(7%)	

A. Security Awareness based on gender

To understand and compare the security awareness about the existing security features, we performed a statistical test (i.e., Independent Sample T-test) to show if there was a significant difference between male (n=61) and female (n=40) respondents. The result indicated that there was no significant difference (i.e., variances are equal, H0: µ1= µ2) between male (M = 3.627, SD =.766) and female (M = 3.634, SD

=.638) (t= -.049, p-value= .961), as in Table 6.2. Thus, we concluded that both males and females in our sample have equal security awareness towards the existing features.

B. Security Awareness based on IT knowledge level

We conducted the Kruskall-Wallis H test to examine if there were any significant differences in the security awareness of the existing security features among the three groups (i.e., Little or no knowledge, Moderate knowledge, and Advanced knowledge) as in Table 6.2. Our findings suggest that security awareness differed significantly (p=0.006). For Advanced IT knowledge, the mean rank = 33.81 which is less than the mean rank = 52.78 for Moderate IT knowledge and less than Little or no knowledge (mean rank = 59.84). Specifically, significant differences were found (using the post-hoc Mann-Whitney U Test) between the Little or no knowledge group compared with the Advanced knowledge group (p =.003). In addition, we found that there was a statistically significant difference in security awareness between the Moderate knowledge group, and the Advanced knowledge group (p=.010). On the other hand, we found that there was no statistically significant difference in security awareness between the Little or no knowledge group, and the Moderate knowledge group (p=.256). Overall, we observed that end-users with Advanced knowledge of IT had higher security awareness scores, compared to those who had Moderate knowledge, or Little or no knowledge. Therefore, we reject H0 and accept H1 concluding that IT knowledge level had an impact on the security awareness of our respondents.

C. Security Awareness based on age group

We conducted a Kruskall-Wallis H test to determine any significant difference among the three age groups (i.e., n=33; young adult, n=60; adult, n=8; senior) in terms of their security awareness. To justify the low number of the senior sample (8 out of 101), we noticed during data collection that the majority of seniors (i.e., those above 50) do not use the provided mHealth apps for some reasons (e.g., they did not carry smart phones, even if they have smart devices it is not mandatory to use mHealth apps). Our findings suggest that security awareness for the groups, adult, young adult, and senior adult were mean rank = 46.87, mean rank= 54.85, and mean rank = 66.13 respectively (p=0.14), as in Table 6.2. Since the young adult group had less security awareness than the adult group, we investigated the IT knowledge level of the young adult group (n=33) to elaborate a little bit on these results. We found that 30, i.e., 91% of respondents considered their IT knowledge as either moderate knowledge or little or no knowledge. Therefore, we accept H0: μ1 = μ2 = μ3 and conclude that age has no impact on the security awareness of our respondents.

D. Security Awareness based on level of formal education

We also wanted to investigate respondents' differences by considering the impact of the level of formal education on our respondents. We conducted a Kruskall-Wallis H test on the five groups, which we identified as shown in Table 6.2. Our results indicated that there is evidence (p=0.007) that security awareness of those with a postgraduate qualification (Higher Diploma, Master's or PhD) was lower, in terms of the sum of rank orderings, than those with an education level of Diploma/Bachelor less than High School or less. To further understand the difference between the five levels of education, we conducted a post-hoc Mann-Whitney U test. We found significant statistical differences in the security awareness between the High school or less and Higher Diploma groups (p= .005) and between the High school or less and Master's or PhD groups (p= .007). Further, we noticed a statistically significant difference between the Bachelor degree group and the Higher Diploma group (p= .011). Our analysis also indicated a statistically significant difference between the Bachelor degree group and the Master's or PhD group (p= .024). Therefore, we reject H0: μ1 = μ2 = μ3 = μ4 = μ5 and conclude that the level of formal education has an impact on the security awareness of our respondents.

E. Security Awareness based on the frequency of mHealth app usage

Lastly, we wanted to examine if our respondents' security awareness differed based on their frequency of usage. We conducted a Kruskall-Wallis H test on the obtained responses which were divided into six groups, as in Table 6.2. Our findings indicate that there was no statistically significant difference in security awareness based on the frequency of mHealth app usage (p=.797). Similarly, we examined the security awareness based on the frequency of mHealth app usage through a post-hoc Mann-Whitney U test. We did not observe any significant differences among the six groups. Therefore, we accept H0: μ1 = μ2 = μ3 = μ4 = μ5 = μ6 and conclude that the usage frequency for mHealth apps has no impact on the respondents' security awareness.

6.3.1.3 Desired Security Features in mHealth apps

To understand the second dimension of end-users' security awareness, i.e., the desired security features, we presented an open-ended question (**Q11**, per survey design in Figure 2.3, Phase 1). The question inquired about the security features desired by the users in existing mHealth apps. The open-ended question aimed to capture and compile a wish list that users perceive as vital to further optimize the security features of the mHealth apps they use. Based on users' responses, we identified two desired features, namely usable security and privacy preservation that can be further classified into nine sub-features, as in Figure 6.2. The text from users' responses was analysed to identify recurring themes, i.e., repeated text patterns for classification and generic naming of the features (illustrated in Figure 2.5). Once the generic features were identified, we put specific features of users' responses under fine-grained analysis, discussed in the subsections below. Figure 6.2 complements the discussion of the desired security features based on a relative percentage of the respondents and their preferences for specific features.

A. Usable Security for User Authentication

As in Figure 6.2, 74% of the respondents desired a combination of secure and usable security features for authentication, referred to as usable security for authentication. Usable security refers to human

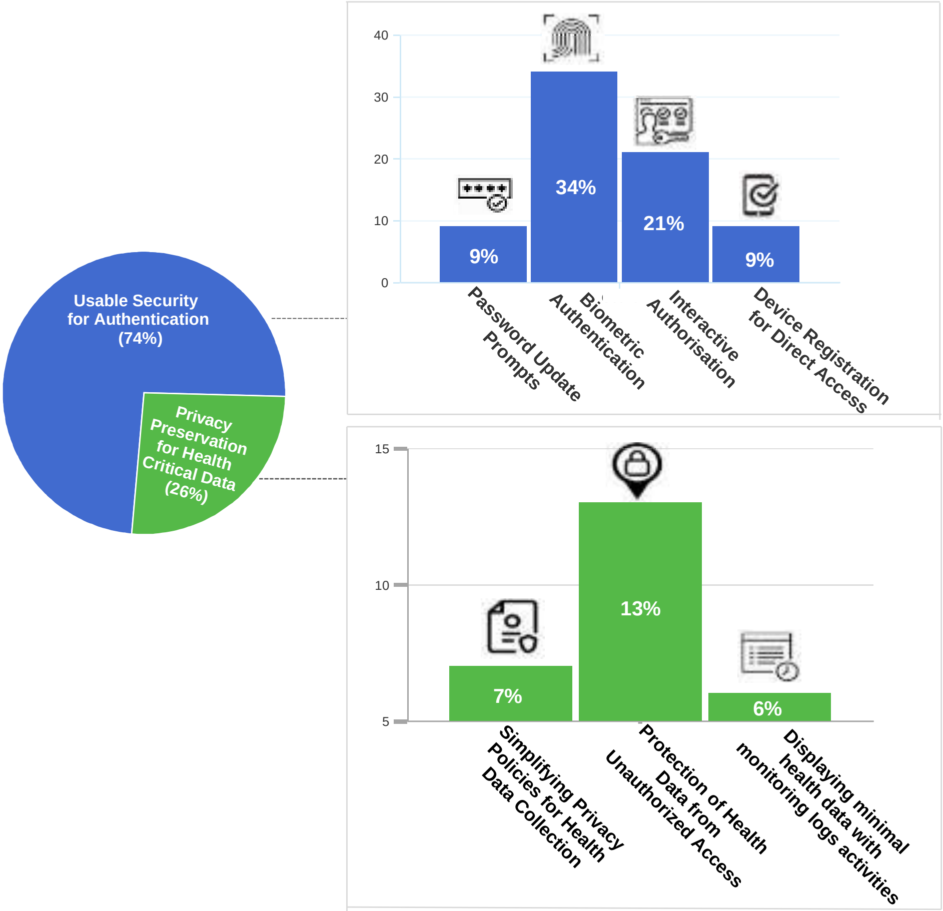


Figure 6.2 Preferred Security Features by our Respondents

aspects and their impacts on computer security, i.e., employing methods of human-computer interaction to support security features that are easy to use [147]. As a typical example, biometric verification is considered a usable security feature (i.e., enabling interactive, easy to use, personalized authorisation) when compared with the traditional ID and code-based authorisation. For a detailed and fine-grained analysis of the desired features, we identified and represented five sub-features of usable security for authentication, each of which is detailed below and illustrated in Figure 6.2. Table 6.3 complements the discussion of ***RQ8*** by highlighting some of the responses from end-users regarding their perception about existing and desired security features.

As in Figure 6.2, 34% of the respondents helped us to identify biometric verification as one of the desired features supporting usable security for authentication. For example, three of the respondents [**R1**, **R20**, **R72**] indicated their desired feature as: 🗨 *'Accessing the app through facial recognition (becomes) easier and faster than using passwords'*[**R1**], 🗨 *'Fingerprint to provide an additional feature for user verification'* [**R20**] and 🗨 *'(I) prefer using a fingerprint to log in'* [**R72**]. We now present the identified sub-features of usable security for authentication, as illustrated in Figure 6.2.

Table 6.3 Example of User Responses (Existing and Desired Features) in the Context of RQ8

Example of End-Users' Responses		**Response ID**
A. Existing Security Features		
App Permissions		
SA-1	*'It is unknown how health data is being handled. But we trust (the health provider) to keep the app secure'*	**R68**
SA-2	*'the app is easy to use for authentication and trusted for not asking my personal information that is not relevant to my health issues and visit to health centre'*	**R36**
SA-3	*'the app does not collect health data and not attached to other devices; all data came from hospital's database'*	**R48**
User Authentication		
SA-4	*'The two-authentication factor is enough to ensure security'*	**R96**
SA-5	*'Provide some instructions for the users on how to create strong passwords'*	**R60**
User Control		
SA-6	*'the app allows me to prevent or permit accessing only my contact and camera'*	**R65**
SA-7	*'(I am) not aware of how (my) health data can be erased from a lost or stolen device'*	**R11**
Feedback and Reporting		
SA-8	*'The app contains an icon to report any issues related eservice including the app'*	**R31**
B. Desired Security Features		
Usable Security		
Password Update Prompts	*'Forcing the user to change the password periodically so it becomes prone to (password) sniffing attacks and only the actual user would access the app'*	**R28**
	'(the app) must support reminders to change the password frequently and accepting strong passwords only'	**R34**
Biometric Authentication	*'The use of the fingerprint is easier and convenient for me but sometimes the verification message arrives too late'*	**R19**
	'Accessing the app through facial recognition easier and faster than using passwords'	**R1**
Interactive Authorisation	*'The app should be accessible by sending a verification code to the registered phone number. Similar to the banking apps'*	**R43**
	'Double confirmation of access password and text code via phone SMS'	**R46**
Device Registration for Direct Access	*'Saving passwords on a registered device and allow users to login directly (with a touch or click) because I would be the only one who uses the mobile after I login to my device'*	**R8**
	'Is it not possible to make the app accessible without re-entering the password as long as the same device remains with the person?'	**R11**
Privacy Preservation		
	'Privacy policy in the app needs to be simple and easy to read for users'	**R24**

Simplifying Privacy Policies for Health Data Collection	*'Al Habib App stores many personal data about the users. The privacy policy is not clear on how to deal with data'*	**R67**
Protection of Health Data from Unauthorised Access	*'My health information should not be disclosed without my permission and should not be shared with private clinics for the purpose of sending offers for me'*	**R83**
	'The user should be informed about any data access, Notify access alert through application or SMS'	**R64**
Displaying minimal health data with monitoring logs activities	*'The app should not display too much health information when it is not useful to display'*	**R52**
	'They should introduce a facility to review my profile access, including the lab results with access time and the requester information'	**R64**

- *Password Update Prompts:* It refers to a commonly implemented feature that frequently notifies the user to update their passwords and/or help them select passwords based on specific character combinations to increase the password strength. As per Figure 6.2, 9% of the respondents suggested that mHealth apps should encourage end-users to change their passwords frequently and facilitate them about how to create strong passwords. For example, as in Table 6.3, the responses [**R28**] and [**R34**] indicated that the app should force users to regularly update their passwords to avoid password breaching.

– *Biometric Authentication*: It refers to exploiting the unique features of human biometrics such as fingerprints, facial imaging, or retina imprints to enable user authentication. Compared to others means of authorisation and authentication, biometric authentication is the most desired feature suggested by 34% of the respondents. Some example responses such as [**R1**] and [**R19**] suggested that finger printing or facial recognition is an easier, faster, and foolproof way to log in to the mHealth app. *'Accessing the app through facial recognition is easier and faster than using passwords'* [**R1**], and *'Use of a fingerprint is helpful to login but sometimes the verification text arrives too late …'* [**R19**].

– *Interactive Authorisation:* It refers to prompting for further input to grant the user access to resources (e.g., 2FA) [148]. 21% of respondents preferred interactive authorisation in mHealth apps. Respondents (e.g., [**R15**], [**R43**], [**R46**], [**R80**], [**R96**]) pointed out that mHealth apps should be accessible after verifying the user. *'The app should be accessible by sending a verification code to the registered phone number, similar to my banking app'* [**R43**].

– *Device Registration for Direct Access:* It refers to registering a device that can access the app installed on a device without any further authentication. This means that once the authorised user logs in to the device, he can directly access the mHealth app, a feature desired by 9% of the respondents. The users indicated that having a registered device makes it more convenient and faster to log in [**R8**], whereas [**R11**] suggested he/she finds repeated logins as inconvenient and exhaustive and prefer an authorised person to access any app directly once logged in to their device. *'Saving passwords and allow users to login directly because he or she would be the only one who uses the mobile'*[**R8**], and *'Is it not possible to make the app accessible without re-entering the password as long as the same device remains with the person?*' [**R11**].

Based on user responses, we observed that the majority of end-users desired convenience and ease of use, fewer steps to log into the examined apps and access their private health-critical data. Based on the percentage of users in Figure 6.2 and example data in Table 6.3, we can conclude that respondents on one hand desired simplifying the current authentication methods to access the app, and on the other hand, suggested further restrictions to access the app such as multi-step authentication. In fact, it can be a daunting task to satisfy all end-users requirements for data access. One possible solution, as indicated by a few respondents, is that mHealth apps should enable users to select and configure the authentication method they prefer. For example, the app should allow users to select whether they would like to log in such as, biometrics, or device registration as indicated by [**R28**, **R68**, **R83**, **R101**].

B. Privacy Preservation for Health-Critical Data

Protecting the privacy of health-critical data and private information of users by employing various privacy-preserving methods is desired by 26% of the users, as in Figure 6.2. For example, [**R70**] indicated, *'The app should have complete confidentiality of the patient's health and other private data'*. It should be noted that privacy-preserving for health-critical data overlaps with confidentiality in regards to unauthorised access, health data disclosure, sharing health data [30]. A few respondents were concerned about who accesses their health data (i.e., authorisation). *'Notify access alert through application or SMS'* [**R64**].

Our analysis of the survey responses revealed three features to preserve user privacy in mHealth apps, each detailed below.

– *Simplifying Privacy Policies for Health Data Collection:* Privacy policies refer to statements or a legal formality that details how a mobile app will collect, process, and exchange users' personal information. Privacy policies help users to understand the potential for manipulation of their classified information by an app and any control provided to allow or restrict such access. As per Figure 6.2, 7% of the respondents (e.g., [**R24**], [**R67**]) expressed their concern about the privacy of health data as the privacy policy is not clear in their opinion and hence, they suggested simplifying privacy policies so they could be easily understood. For example, the response [**R67**] suggested that the privacy policy is complex and that it is hard to understand how mHealth apps handle health-critical data. *'(the app) stores many types of personal data about the users. Privacy policy is not clear on how to deal with such data'* [**R67**].

– *Protection of Health Data from Unauthorised Access:* Privacy of health data ensures that classified data is kept private and only shared with entities (e.g., human or computer programs etc.) that are authorised to access it. 13% of the respondents, such as [**R64**], and [**R70**] indicated the features to ensure privacy of their health data and private information. [**R64**] suggested the use of proper notification or alerts in the case of private information being accessed by any third party. *'Notify access alert through application or SMS'* [**R64**].

– *Displaying minimal health data with monitoring logs activities*: Minimal data display ensures that only the most relevant information is shown via an app even to the authorised person viewing it. This means that a clinical technician that needs to pass on a patient's information to a doctor must not be provided with insights into a patient's health conditions and disease symptoms, unless explicitly required. In addition, monitoring logs (audit logs) help to trace unusual access patterns that can be restricted in the future. Some of the respondents suggested complementary audit logging feature to capture and review account activities. 6% of our respondents suggested displaying fewer health data and monitoring who accesses their data. For example, respondent [**R52**] suggested that mHealth app should not display too much health information when it is not required. *'The app should not display too much health information when it is not useful to display'* [**R52**]. Respondent **R64** indicated that the app should provide the facility to review a user's profile access time and the requester information. *'They should introduce a facility to review my profile access including the lab results with access time and the requester information'* [**R64**].

We conclude that end-users were concerned about their privacy and suggested further mechanisms to preserve the privacy of their health-critical data, as shown in Figure 6.2 and example data in Table 6.3. The respondents highlighted some issues that needed to be considered to guarantee data privacy. A few features were desired to be implemented including simplifying privacy policies for health data collection, and ensuring that health data to be shared with authorised entities. Furthermore, the minimal health data should be displayed and monitoring log activities to trace abnormal data access.

6.3.2 Security Related Issues in mHealth Apps (RQ9)

We now answer ***RQ9*** which aims to investigate the security issues faced by end-users while utilising the mHealth apps (i.e., **Q12**, per survey design in Figure 2.3, Phase 1). In our context, we define a security issue as a problem or a challenge experienced by end-users related to security features or other aspects of the app while using the app; for example, requesting permission to access more device resources (e.g., mic or camera) or data (e.g., contacts or photos) than the app actually needs. Based on the collected responses, we identified a multitude of security-related issues ranging from concerns about multi-step authentication to discomfort with sharing health-critical information with stakeholders. The reported issues can provide guidelines to further optimize security and usability of mHealth apps. We also observed that several end-users were not able to point out any security-related issues due to their lack of knowledge (security perception **RQ8**). For example, one of the respondents indicated that: 🗨 *'I have not encountered any (security) problems but my mHealth app provides appropriate security measures to protect my data'* [**R33**].

Some respondents indicated miscellaneous issues that can be classified as generic or performance-related issues such as 'app freezing' 'poor quality of medical imaging', 'lack of notifications' reported by the respondents [**R5**], [**R6**], [**R37**], [**R71**], [**R95**] which were not relevant to app security and were discarded during analysis (as in Figure 2.5). We classified the reported issues into three main categories as in Figure 6.3, each of which is detailed below. Table 6.4 complements the discussion of ***RQ9*** by highlighting some of the responses from end-users regarding the security issues in mHealth apps.

6.3.2.1 Delays in Two-Factor Authentication (2FA)

Difficulty or delays in authenticating an app's users can be related to the issues in the execution of security procedures that are responsible for gathering users' credentials to verify and authenticate for system login. The primary issue reported in this context is 2FA that first collect users' credentials and then authenticates them via an SMS to the registered device or telephonic number.

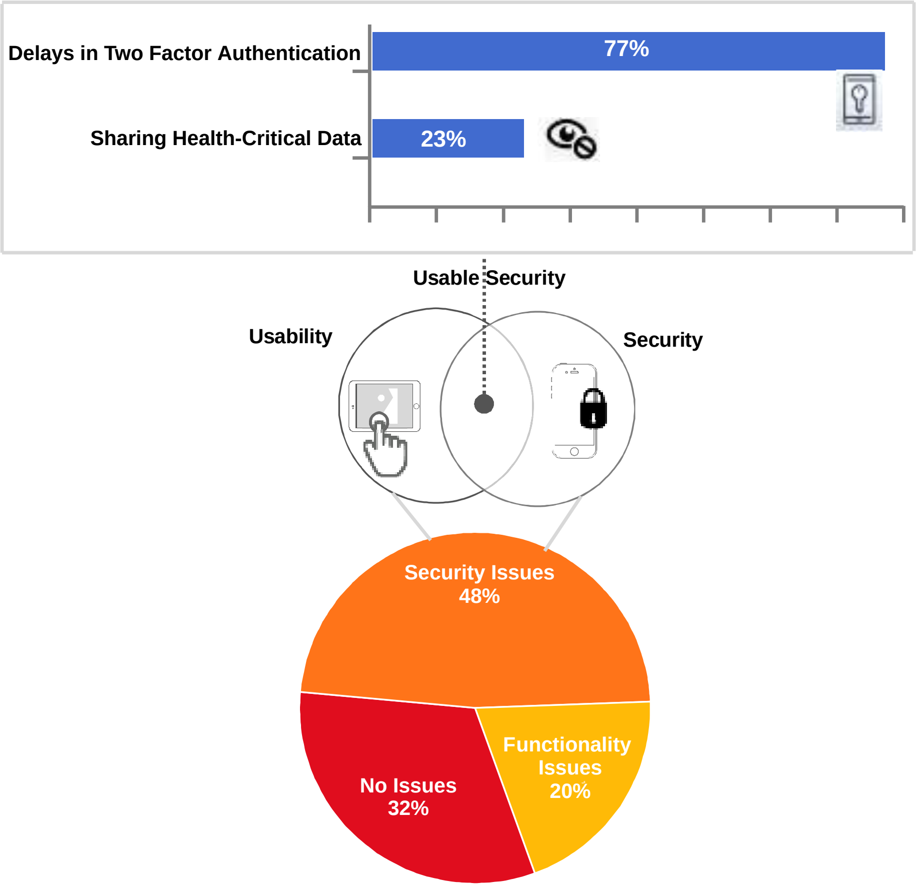


Figure 6.3 Security Issues with the Examined mHealth Apps by our Respondents

Security regulations and policies such as HIPAA and EU GDPR recommend the implementation of 2FA features for ensuring the security of mHealth apps by adding an extra layer of authentication on top of traditional identity and passcode-based access [26, 28]. However, the respondents indicated that such a delay in getting the verification code would affect the usability of the apps. 2FA enhances an app's security but can restrict a user from entering the app if the SMS is not delivered due to network or connectivity issues. For example, several respondents (e.g., [**R2**], [**R18**], [**R19**], [**R54**], [**R56**], [**R57**], [**R92**]) reported that the delays in getting the app verification code in some instances lead to session expiry. Specifically, two of the respondents suggested that 🗨 *'Sometimes verification message is not received in a* *timely fashion and I cannot get (into) the app"* [**R18**], and, *'Due to weak network signals, sometimes I do not timely receive the SMS to change my password'* [**R43**].

6.3.2.2 Sharing Health-Critical Data with Stakeholders

Securing private data and ensuring its privacy from other humans or non-humans such as third-party programs that sense users' location and context is a critical concern for end-users. The survey findings indicate that some of the users are uncomfortable with the fact that all medics (manager level users of the app, e.g., nurses, doctors, technicians), regardless of their medical relevance can search and view health-critical information of any patient. Furthermore, the access privileges for managerial level users of apps can be extended beyond the working hours and health unit premises. This raised concerns about privacy of users' health-critical data (disease symptoms, medical images etc.) that can be leaked and have specific social consequences. For example, respondent [**R52**] indicated that: *'Health information should remain between doctor and patient and should not be shared outside the hospital. They (the medics) have the access to patients' data, and they can share my information with others without my consent or any alerts from the app'*. The user should be able to give consent to access health data as [**R24**] suggested. [**R24**] indicated: *'The medical record can be accessed after obtaining approval from the user and it is in the form of a code sent as a text message on his/her mobile'*. Specific concerns for data privacy included using personal information for advertising purposes. [**R83**] indicated that: *'The app should not display too much health information when it is not useful to display'*.

Table 6.4 Example of User Responses (Security Related Issues) in the Context of RQ9

Example of End-Users' Responses	**Response ID**
A. Delays in Two Factor Authentication	
'Sometimes verification messages not received in a timely fashion and I cannot get (into) the app'	[**R18**]
'Due to weak network signals, sometimes I do not timely receive the SMS to change my password'	[**R43**]
B. Sharing Health-Critical Data with Stakeholders	
'Health information should remain between doctor and patient and should not be shared outside the hospital. Doctors have access to their patients data and they can share my information with others'	[**R52**]
'My health information should not be disclosed without my permission and should not be shared with private clinics for the purpose of sending offers for me'	[**R83**]

Developing secure mHealth apps requires following a certain guideline, such as HIPAA, to ensure the security expectations are met. However, as illustrated in Figure 6.3 and example data in Table 6.4, some of our respondents found some of the employed features challenging. Our respondents indicated that 2FA through messaging a code via SMS can cause difficulties in accessing mHealth apps. Even though 2FA provides an extra layer of protection, it needs to be more convenient for end-users. Also, the respondents pointed out that health professionals should keep end-user's data confidential. It would be possible to obtain end-users' consents through mHealth apps once sharing health-critical data with other health professionals is required.

6.3.3 Methods to Improve Security Awareness (RQ10)

We now answer ***RQ10***, which aims to identify the methods and practices adopted by end-users or supported by mHealth providers to improve the security awareness of end-users (i.e., **Q13,** per survey design in Figure 2.3, Phase 1). Earlier studies such as [4, 15] indicate that developing secure apps or adopting state-of-the-art security practices may not be sufficient to protect the classified data of end-users. End-users' awareness in terms of their knowledge, attitude, and behaviour to identify threats and adopt security-aware practices for their private and health-critical data is of prime importance [114, 149]. For example, despite advanced data encryption techniques for medical records (i.e., technical perspective), the selection of a weak password scheme or infrequent update of it (i.e., human perspective) may expose users' data to vulnerabilities [22, 24]. Therefore, educating users or employing methods that enhance their understanding of security is important for mHealth providers to avoid any socio-legal challenges of security breaches [23, 40]. Based on the survey responses, we have identified and classified the reported methods that help end-users to improve their security awareness. First, we have analysed the text of the survey responses to identify two categories: (i) end-users that self-educate and (ii) end-users that need support from app providers to improve their security awareness. Figure 6.4 visualizes both of the categories for fine-grained discussion of methods that improve security-awareness of end-users. We excluded comments that were based purely on user awareness about app usability with no link to security. Table 6.5 complements the discussion of ***RQ10*** by highlighting some of the responses regarding the methods that help end-users to improve their security awareness.

6.3.3.1 Self-Education

As in Figure 6.4, 32% of end-users indicated that they self-educate to improve their security awareness about the mHealth app. For example, the respondents (e.g., **[R11]**, **[R14]**, **[R23]**, **[R31]**, **[R48]**) indicated that they relied on themselves to explore security features or read the apps' manuals. Based on the demography analysis (Figure 2.4), we observed that almost all of the respondents opting for self-education have at least a bachelor's degree with moderate to advanced knowledge of IT. For instance, **[R14]** wrote, 🗨 *'I learned about the app by myself and by practising'*. Moreover, some of the respondents (e.g., **[R23]**, **[R31]**, **[R44]**, **[R50]**, **[R56]**) indicated that they had not been guided about secure usage of the apps or about utilising the specific security features of the app but they were motivated to learn about usability, functionality, and security. For example, the respondents **[R44]** and **[R68]** suggested that exploration of the app's functionality and excitement about learning features to secure their personal data helped them to learn about the security features provided by the app.

6.3.3.2 Support from App Providers

As in Figure 6.4, 68% of the end-users indicated the need for support from app providers to improve the security awareness of end-users. For example, some respondents including **R21**, **R60** suggested further support from the app provider to educate users about protecting their data. For example, **R60** wrote, 🗨 *'(the app provider should provide) some instructions to the users such as how to create strong passwords or manage app access permissions'.*

Based on end-user responses, the methods provided by app providers can be generally divided into three main categories, each of which is detailed as below and illustrated in Figure 6.4.

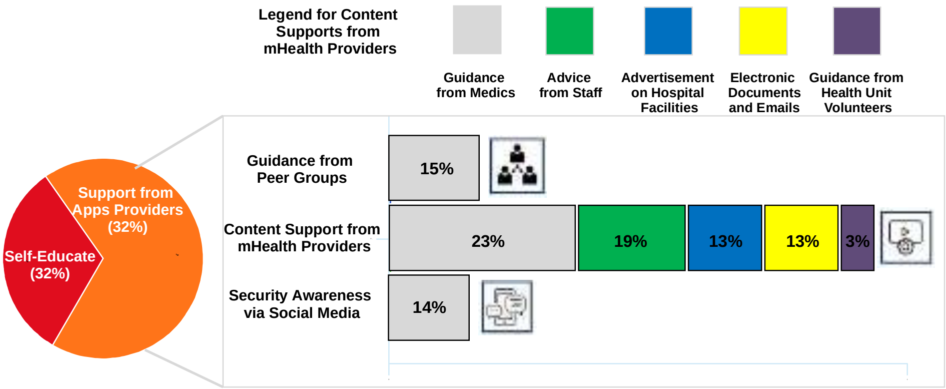


Figure 6.4 Methods to Improve End-users' Security Awareness by App Providers

Table 6.5 Example of User Responses (Methods to Improve Security Awareness) in the Context of RQ10

Example of End-Users' Responses	Response ID
A. Self-Education to Improve Security	
'The app is easy-to-use and does not need much awareness about its use and steps for changing my password or deny (requested) permissions'	[R11]

B. Support from App Providers to Improve Security Awareness		
Security Awareness via Social Media		
'I watched a short video on Youtube about how to securely setup (and configure) my app'		[R12]
Contents Provided by Health Provider		
Guidance from doctor or nurse	*'My doctor advised me to download, and he showed me how to use the existing features'*	[R4]
Advice from staff	*'While booking an appointment, a brief introduction of the app was given to me including password creation and accessing my data securely'*	[R88]
Advertisements on hospital facilities	*'The interactive screens inside the buildings assisted me in learning about the app and made me realise about security of the data'*	[R17]
Receiving Support E-mails	*'I learned the security features through the frequent e-mails which I receive from the health provider to guide me on how to use the app'*	[R10]
Support from hospital volunteer	*'The app was presented to me [...] through a volunteer team to help me understand its usage and basic security features'*	[R100]
Guidance from Peer-Groups		
'My younger brother recommended and downloaded the app for me. He helped to sign up and showed me how to use it and keep it secure'		[R25]

- *Security Awareness via Social Media:* As in Figure 6.4, a total of 14% of end-users suggested that they become security-aware via social media. As per some respondents **[R12]**, **[R16]**, social media campaigns, documentary tutorials, and videos help end-users to view, share and engage in discussion regarding various aspects of the apps that they use. The respondents indicated that social media presence of the mHealth app providers helped them to get useful information and query needed clarifications. For example, three respondents (i.e., **[R12]**, **[R16]**, **[R71]**) indicated that posting on a prominent social media platform like Twitter and uploading a tutorial video on YouTube have helped them to learn about the app security features. For example, **[R12]** wrote, *'I watched a short video online about how to securely setup (and configure) my app'*.

- *Content Support from mHealth Provider:* Figure 6.4 suggests that an overwhelming majority of users (i.e., 71%) indicated that they rely on the content from the mHealth providers to improve their security awareness. mHealth providers provide different types of content such as guidance from app experts to be consulted, email, helpline and support. 22 respondents (e.g., **[R4]**, **[R13]**, **[R26]**, **[R34]**, **[R100]**) reported that they have been notified of the security features by health providers' channels, which can be classified into five main types

a. Guidance from doctors or nurses (23% respondents): Some of the respondents (e.g., **[R4]**, **[R6]**, **[R15]**, **[R4-6]**, **[R9]**) indicated that the assigned doctors or nurses showed them how to use the app. *'My doctor advised me to download, and he showed me how to use the existing features'* **[R4]**.

b. Advice from staff (19% respondents): The respondents (e.g., **[R26]**, **[R29]**) in this category indicated that medical support staff such as reception or helpdesk personnel helped them to familiarize themselves with the usability and security features of the app. *'While booking an appointment, a brief introduction of the app was given to me including password creation and accessing my data securely'* **[R88]**.

c. Advertisements on hospital facilities (13% of respondents): The respondents (e.g., **[R17]**, **[R55]**) indicated that the facilities and interaction on hospital premises helped them understand the importance of securing health data and personal information. *'The interactive screens inside the buildings assisted me in learning about the app and made me realise about security of the data'* **[R17]**.

d. Electronic Documents and Emails (13% respondents): The respondents including **[R10]**, **[R34]** pointed out that they learned about the security features of the app based on materials shared via electronic mail. *'I learned the security features through the frequent e-mails which I receive from the health provider to guide me on how to use the app'* **[R10]**.

e. Guidance from Health Unit Volunteers (3% respondents): Only a minority of the respondents (using the KFMC app) indicated that meeting a volunteer helped them become aware of the security features. *'The app was presented to me [...] through a volunteer team to help me understand its usage and basic security features'* **[R100]**.

- *Guidance from Peer-Groups:* Peer groups of mHealth app represent a group or circle of friends who use mHealth apps like family contacts or colleagues. Figure 6.4 highlights a total of 15% of end-users that rely on guidance from peer-groups for security awareness. Specifically, five respondents (e.g., [**R3**], [**R7**], [**R25**], [**R72**]) indicated that they have appropriate knowledge about using the app securely and it is observed that the improved skills are the result of respondent's consultation with a friend, family member or colleague at work. *'My younger brother recommended and downloaded the app for me. He helped to sign up and showed me how to use it and keep it secure'* [**R25**].

Based on the discussion above regarding the approaches to improve users' security-awareness, we conclude that end-users have not received sufficient awareness training on how to use mHealth apps in a secure way, as in Table 6.5 and Figure 6.4. Even though 83% of our respondents relied on the content from the mHealth providers, we argue that the objective was more about marketing the app rather than providing security awareness. We believe that end-users should be further assisted through providing security training. Such training should be delivered through security experts to ensure end-users become aware of security threats and the appropriate mechanisms to manage risks.

6.4 Discussion of the Key Findings

Our study empirically investigated the security awareness of end-users about using clinical mHealth apps. We presented our findings based on participants from our case health providers. While it can be argued that some of the recommendations and guidelines presented in this study are applicable to other mobile apps, the outcomes represent the participants' views. Deciding what security features should be employed in mHealth apps rests upon health providers. We now discuss the key results that highlight the core findings for ***RQ8 – RQ10*** based on methodological steps in Figure 2.3, and outline the scope for future work. The discussion is guided by Table 6.5 which provides an illustrative summary as a taxonomy of the key results. Based on Table 6.5, first, we highlight the demography and app usability analysis (Section 6.4.1) followed by a summary of answers to RQs (Section 6.4.2– Section 6.4.4). For example, Table 6.5 highlights that, in the context of ***RQ9***, biometric authentication is a desired feature of usable security. As explained earlier, several respondents desired biometric authentication (e.g., facial recognition) as a more user-friendly and faster mechanism to access the app compared to typing ID and password.

6.4.1 Demography and App Usability Analysis

The demography analysis helped us to investigate if factors like users' experience, education or IT proficiency impact their security awareness and reflect any patterns for secure usage. For example, the respondents such as [**R11**] and [**R14**] (who have bachelors' degrees and knowledge of IT) pointed out that their concerns about the security of their data motivated them to self-educate about the app's security (***RQ10***). In comparison, some respondents such as [**R66**] (with a high school degree and minimal to no knowledge of IT skills) were not sure about the features offered by the app for data security. The study acknowledges that some of the received responses focused solely on app usability and security-specific issues, since most of the respondents lacked IT knowledge or experience with mobile app usage. Such analysis provides a fine-grained investigation of end-users to analyse if education, IT proficiency and usage history impacts end-users' awareness, and ultimately increase the security of their health-critical data.

Based on the survey responses, 95% of our respondents believed that the security of their private information (e.g., location, age, gender) and health data (e.g., blood pressure, medical history) is a critical concern to them. Specifically, 88 respondents (i.e., 87.1%) selected very important, eight of them selected important (7.9%), and a further four (4%) remained neutral, as highlighted in Figure 6.5. Surprisingly, one of the respondents indicated that the security of mHealth apps is not important at all as (s)he considers it valuable if the app enables her/him to share his/her health and fitness routine with his social media contacts. Specifically, the respondent [**R8**] suggested that *'I use (…) app for consulting (the nutritionist) regarding my diet and fitness monitoring and security of my (dietary, exercise, fitness monitoring, etc.) data is not very critical. I would prefer if it allows me to share my workout, diet plans and recommendations from the doctor (i.e., nutritionist) can be read and automatically shared with my (social* *media) friends and contacts. I will not be comfortable sharing my (exact) location but other than that if the app shares my (fitness) data with my permission, I am OK with that.'*

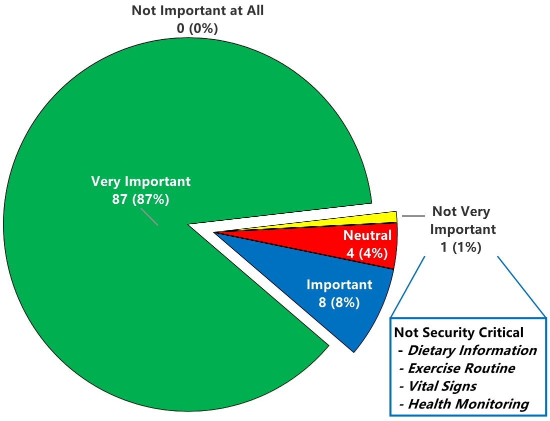


Figure 6.5 Respondents' Perceived Importance of Securing Private Data within the Apps

The findings indicated that the vast majority of our respondents (95%) are concerned about securing their health-critical data. Only 1% was less concerned about health-critical data that corresponds to health and fitness monitoring.

6.4.2 End-users' Understanding of Existing Security Features and the Desired Security Features

Security perception of end-users is indicated based on their understanding of the existing features (Figure 6.1) and the knowledge about the desired features (Figure 6.2) that enable or enhance app security. The key findings indicate that majority of the end-users were unaware of the security features that had been implemented in the app they were using (Figure 6.1). For example, 26.7% of our respondents were aware that the mHealth apps have very adjustable security settings that help to control apps permissions. The findings suggest that end-users find it impractical to have apps that offer a multitude of security features that are difficult to understand or use.

The respondents indicated a total of seven desirable features that support (i) usable security for authentication (i.e., 74% end-users) and (ii) privacy preservation (i.e., 26% end-users), as illustrated in Figure 6.2. For example, Device Registration for direct access to app data is the desired feature as indicated by [**R43**]. 43% of the end-users liked the security features such as biometric authentication, or device registration for user authentication.

Our study revealed that the respondents did have concerns about the security and privacy of their health-critical data. At the same time, we found out that the majority of our respondents are still not fully aware of the employed security features that help to control mHealth apps. In fact, [**R21**] suggested that there is a need to raise awareness about using mHealth apps. Because mobile devices are more vulnerable to security breaches, there is a clear need to ensure that end-users are familiar with basic security features which protect their critical data in order to enhance app security, and increase and increase users' trust in using the app. In particular, the use of BYOD has the potential to damage/ compromise security since mobile devices run other mobile apps, which frequently access device data, in parallel to mHealth apps. As a result, lack of security awareness can compromise the security and privacy of health-critical data. We also identified seven security and privacy-related features based on the surveyed end-users. Our findings can be useful for mHealth app developers to consider the identified security features as guidelines and recommendations. More importantly, convenient apps need to ensure a tradeoff between security and privacy, on the one hand, and mHealth apps usability on the other hand.

6.4.3 Security Specific Issues Faced by End-Users

The respondents were asked about the security-related issues that they experienced while using the security features in the examined mHealth apps. Our study confirmed that the examined mHealth apps still have some security issues that our respondents have experienced. Our findings are consistent with those of previous studies (e.g., [23, 24, 53]) regarding the security issues faced by end-users. As in Figure 6.3, 48% of the respondents reported usable security issues faced by them that affect user experience or discomfort about app usage. Implementing the 2FA to access mHealth apps aligns with one of the recommended security practices by health regulations (e.g., HIPAA). However, it limits end-users to a specific authentication method, which sometimes does not work well (e.g., due to weak cellular network signals) and can affect the availability of the apps. Another security concern mentioned by our respondents is the violation of end-user's privacy (Figure 6.3) by managerial level users of the app e.g., nurses, doctors, technicians. Some respondents indicated that medics can access and share their health-critical data without getting consent from end-users.

In summary, our findings presented end-users' evaluation and suggest a few security measures that would provide more secure, effective, and convenient mHealth apps. First, issues during authentication were the most indicated by our respondents, and better authentication methods, the most desired features. Therefore, we conclude that following HIPAA regulations, i.e., selecting two of the three recommended authentication methods: i) something an end-user knows (e.g., ID and passwords), ii) something an end-user owns (e.g., authentication tokens), or iii) something an end-user finds most convenient (e.g., biometric authentication) would increase end-users' trust in using mHealth apps, and enhance the security. On the other hand, ensuring the privacy and confidentiality of users' health data was a big concern for a few respondents. For instance, unnecessary authorisation, especially for different units of the health providers, can lead to exposure to health data. Thus, suitable privacy-preserving methods, such as anonymization, could be employed by the developers to enhance end-users' use of mHealth apps. Furthermore, health data should be subject to a proper access control policy (i.e., notifying end-users who accesses their health-critical data, when, and for what reasons). We believe our results can help guide the development team to incorporate better security features.

6.4.4 Methods to Improve Security Awareness of End-Users

Raising the security awareness level of end-users towards using mHealth apps is crucial for health providers to avoid security risks. As illustrated in Figure 2.3, ***RQ10*** aimed at investigating how end-users of mHealth apps become aware of the security features offered by the apps. On the one hand, 32% of our respondents (e.g., [**R11**], [**R14**], [**R23**]) preferred self-education to improve their security perception (Figure 6.4). Demography analysis suggested that almost all such respondents that advocate self-learning and education have an appropriate level of IT knowledge or they have installed and used similar apps (e.g., other health provider apps) on their devices. On the other hand, 68% required help and support via social media (e.g., [**R12**], [**R16**]), through the content provided by the health providers (e.g., [**R4**], [**R26**]), and/or needed guidance from peer-groups (e.g., [**R3**], [**R25**]) to improve their security awareness. Security awareness towards using mHealth apps is getting the attention of end-users and they welcome any opportunity to be educated.

To summarize, providing security awareness for end-users is just as important as developing secure mHealth apps. There is a need for suitable security awareness methods supported by internal security experts to help end-users to avoid security-related risks. 42% of the respondents, such as [**R9**], [**R15**], [**R26**] indicated that medics or staff members had helped them in some way to become more aware of the apps, as in Figure 6.4. It would be quite helpful to organise short sessions to enable medics and staff members to be fully aware of all security aspects of the provided apps to ensure that end users are educated with appropriate security awareness. Such training could be arranged through a guidance program with each unit assigning a person to teach others within the unit to overcome the large numbers of participants.

Table 6.6 Taxonomical Classification of the Core Findings (Key Results for all RQs for Chapter 6)

App Usability Analysis						
Mobile Platforms	Used app	Gender	Age Group	IT Knowledge Level	Education Level	App Usage
• 33% Android • 66% iOS • 1% Meizu	• iKFMC App (62%) • Dr. Sulaiman Al Habib app (38%)	• 41% Female • 59% Male	• 33% 18 – 29 years • 59% 30 – 49 years • 8% Above 50 years	• 31% Little/no knowledge • 48% Moderate knowledge • 21% Advanced knowledge	• 11% High school or less • 13% Diploma • 45% Bachelor • 10% Higher diploma • 22% Master's or PhD	• 6% At least once a day • 14% At least once a week • 37% At least once a month • 23% At least once every 3 months • 14% At least once every 6 months • 7% At least once a year

Security Perception (RQ1)						
Securing Health Data	Security Awareness				Desired Features	
The importance of securing health data within mHealth apps	**App Permissions**	**User Authentication**	**User Control**	**Feedback and Reporting**	**Usable Security for Authentication (74%)**	**Privacy Preservation (26%)**
• **87.1%** believed it is very important • **7.9%** believed it is important • **4%** of respondents were neutral • **1%** believed it is not important	User Consent: **20.8%** were unaware if the apps require users consent or not.	2-Step Authentication: **24.8%** were unaware if the apps support 2-step authentication or not.	Adjustable Security: **48.8%** were unaware if the apps have adjustable security or not.	Backend Security: **46.5%** were unaware if the apps have the feature of reporting security issues or not.	• Password Updates (**9%**) • Biometric Authentication (**34%**) • Interactive Authorisation (**21%**) • Device Registration for Direct Access (**9%**).	• Simplifying Privacy Policies (**7%**) • Protection of Health Data from Unauthorised Access (**13%**) • Displaying minimal health data with monitoring logs activities (**6%**)
	Information Access: **40.6%** were unaware if the apps collect data without permission or not.					
	Data Collection: **61.4%** knew that the apps don't collect more personal information.	Password Strength: **35.6%** were unaware if the apps accept weak passwords or not.	Data Wiping: **60.4%** knew that the apps have the data wiping feature.			

Security Issues (RQ2)	Security Education (RQ3)
Security issues that end-users faced during their usage of the employed security features within mHealth apps. • Delays in authentication (**77%**) • Sharing their health data (**23%**)	**Methods that improve the security knowledge of end-users towards using mHealth apps.** • Self-education (**32%**) • Support from app providers (**68%**) is as follows: - Guidance from peer groups (**15%**) - Security awareness via social media (**14%**) - Content support from mHealth provider (**71%**) including a. Guidance from doctors or nurses (**23%**) b. Advice from staff (**19%**) c. Advertisements on hospital facilities (**13%**) d. Electronic Documents and Emails (**13%**) e. Guidance from Health Unit Volunteers (**3%**)

6.5 Related Work

There are a number of studies including [23, 24, 40, 53, 115], which investigated end-users views on the security of mHealth apps that inspired the work presented in this chapter. We now position the reported work with respect to the most relevant studies.

The study by Atienza et al. in 2015 [24] investigated end-users' perceptions and attitudes about the security of mHealth apps. End-users' perceptions and attitudes were highly contextualized based on the type of data collected by an app, time and context of access, i.e., who accessed the data, at what time they accessed it, and why. Alternatively, some end-users do not mind sharing their health-specific data on social networks, gathered by health and fitness monitoring apps (e.g., workout, walking distance, and burnt calories). However, one of its limitations is examining end-users' views about mHealth apps including fitness apps. A research by Peng et al. in 2016 [53] affirmed that one of the barriers to continuing to use mHealth apps is sharing personal information that might be exploited by a third party (e.g., insurance companies or advertisers). Yet, the study indicated that one of the limitations that could affect the results was recruiting participants without prior experience in using mHealth apps.

The study by Zhou et al. in 2018 [115] examined whether a brief security education offered in a mHealth app (i.e., Security Simulator app) can change end-users' security behaviour in terms of choosing appropriate security settings. The participants were asked to make security selections in the developed app before and after they viewed the consequences of security features. The study concluded that simulation-based education is helpful in changing end-users' security behaviour and helps them to select stronger security measures. However, the study was limited to a specific group of end-users, i.e., young and highly educated (Bachelor's degree or higher). The level of satisfaction could be different based on demographic characteristics. Zhou et al. in 2019 [23] identified the desired features of mHealth apps which would enhance the trust of end-users. The participants agreed that their confidence level increases when using mHealth apps that enable end-users to adjust security settings, enforce regular updates for passwords, and allow monitoring data access via access logs. Moreover, the participants suggested biometric verification, providing end-to-end encryption for data-in-transit and data-at-rest, and allowing end-users to wipe the device remotely, once it is lost or stolen. Nevertheless, the study was limited to young users.

A recent study by Aljedaani et al. in 2020 [40] investigated the security awareness of end-users about using clinical mHealth apps. The study was conducted by surveying 101 participants to measure the participant's security Knowledge, Attitude, and Behaviours (i.e., the KAB model that underpins the Human Aspects of Information Security Questionnaire, HAIS-Q). The findings of the study suggested that end-users' security knowledge strongly influence their attitude about the security of mHealth apps. This means that users were aware of risks (e.g., stealing/tempering of health-critical data) and like to mitigate them (e.g., app support for data encryption). The study also revealed that end-users' security knowledge did not significantly influence their behaviour. This indicates that users were aware of risks (e.g., private data shared with third parties for targeted ads) but are reluctant or unaware of appropriate actions that mitigate risks (e.g., setting privacy preferences to restrict undesired data access). However, the study results were based on collecting quantitative data only.

The scope of the presented work in this chapter was precise in terms of investigating clinical mHealth apps such as patient management systems that handle highly sensitive health-critical data and personal information. The study provided an in-depth view of the security awareness of end-users through evaluating the relationship between end-users' security awareness and their characteristics and by identifying specific security features that may enhance end-users' confidence in using mHealth apps, as in ***RQ8***. We also determined the various security-related challenges faced by end-users and their impact on data privacy and the usability of apps, as in ***RQ9***. Furthermore, we presented the implemented methods to ensure end-users have the underlying knowledge of the mHealth apps they use, as in ***RQ10***.

6.6 Conclusions and Future Work

mHealth apps have been gaining more attention recently because they provide innovative solutions to deliver health services. However, despite their promising benefits, mHealth apps are susceptible to many security threats that jeopardize end-users' health-critical data and personal information. We conducted a case study to understand the security knowledge and perceptions of the end-users of mHealth apps. We used a survey method to collect, analyse, and document the end-users' responses. The survey questionnaire was completed by 101 respondents, who were using mHealth apps provided by two approved mHealth providers in Saudi Arabia. Our data collection was enhanced by the demography data of the respondents, which helped us to highlight the supporting factors such as level of IT knowledge, age group, past experience with mHealth apps, mobile platforms they use, and educational backgrounds, that increase our respondent's security-awareness. The key findings of our study are:

- Respondents had significant variances in their knowledge about the existence of the security-related features in the investigated apps.
- Most of the desired security features are related to usable security for authentication and preserving privacy.
- Difficulty in authenticating users, and sharing health data were the reported security issues by our respondents.
- Security awareness towards secure usage of mHealth apps by security experts is missing. Yet, some respondents reported that health providers have supported them to some extent to understand the apps.

This research investigated human-centric knowledge based on empirical evidence and provides a set of guidelines to develop secure and usable mHealth apps. We believe our study uncovered a few implications for future work including:

(i) Helping end-users to understand and prevent any security-related risks while using the apps. Furthermore, the developed security policy and guidelines could clarify the right actions that end-users need to take in different circumstances. At the same time, providing suitable security awareness regarding the policy and guidelines for end-users is as important as developing secure mHealth apps.

(ii) Our study can be further extended to investigate the impact of the desired security features and how that would lead to more secure mHealth apps.

(iii) Future research could investigate the impact of employing strict security features (e.g., employing two-factor authentication). Such an investigation would identify unhelpful security measures, that can be further improved to present usable and secure mHealth apps.

The results of this study can benefit:

- Researchers who are interested in exploring human-centric knowledge for secure development and usage of mobile health applications. The key results streamline potential areas of futuristic research and new hypothesis to be tested in the context of security vs usability of mHealth apps.
- mHealth apps developers and/or stakeholders interested in the fine-grained analysis of security features desired by end-users. In particular, the end-users' perspective could help developers to engineer next-generation of mHealth apps that are secure and usable.

Chapter 7

Investigating Security Awareness of End-Users of Mobile Health Apps: An Attack Simulation Approach

Related publication:

This chapter is based on a manuscript that will be submitted to a suitable journal.

In Chapter 5, and Chapter 6, we investigated the security awareness of end-users when using clinical mHealth apps through a questionnaire-based study. In Chapter 3 (Section 3.3), we reviewed the literature to understand the existing approaches to measure the security awareness of end-users. This chapter presents a user study to measure security awareness through an attack simulation approach, which involved examining the participants' actions to four security threats, specifically access permissions, phishing attacks, and eight security scenarios, such as requesting access to device storage, and clicking on a phishing link. A simulation app was developed and 105 Android users were involved to investigate their security awareness via simulation of security attacks. Whilst the minority of our participants perceived access permissions positively (useful for app functionality), the majority had negative views (fear of data leakage, fear of their devices being hacked, excessive permission triggers a lack of trust, fear of using data for objectionable processing purposes). The results also indicated that participants have given their consent for the simulation app without a careful review of the provided privacy policy, 73.3% of our participants had denied at least one access permission, and 36% of our participants preferred no authentication method. The results of this study can provide guidelines and recommendations that can help app developers and end-user to engineer and utilise mHealth apps securely. As demonstrated in Section 7.3 and outlined in Table 1.1, this chapter focuses on addressing RQ12: How do end-users react while facing potential security threats during the usage of mHealth apps? and RQ13: What security-related mistakes do end-users make while using mHealth apps?

7.1 Introduction

Mobile and pervasive technologies offer end-users a multitude of context-aware services, ranging from social networking, mobile commerce, to smart and connected health care [1, 129]. Mobile health (mHealth) apps, pervasive technologies, and the enabling infrastructures have empowered users and transformed the healthcare sector to provide a wide range of healthcare services. This has resulted in a significant improvement in the mHealth adoption by users (e.g., patients, medics, public health stakeholders), increased effectiveness, and reduced costs for healthcare services [129]. Public and private healthcare providers can leverage mHealth apps to offer digitize healthcare practices such as health and fitness monitoring [5], dermatologic care [6], chronic management [7, 8], and clinical practices [9]. A recent report by Allied Market Research revealed that the global digital health market size was valued at $145,884.3 million in 2020, and is projected to reach $767,718.9 million by 2030 [150].

Despite the potential benefits and strategic importance of mobile technologies and mHeath initiatives in smart systems context, a number of issues such as resource poverty, security of device resources, and privacy of context-sensitive data represent critical challenges to mobile computing solutions. Specifically, the security of mHealth apps is considered a challenge due to the pervasive environment that continuously ingest health-critical data from embedded sensors, processes and persist data inside the device, and transmits it across ad-hoc networks [1, 36]. It has been reported that mobile devices are three times more vulnerable to phishing attacks than personal computers [121]. For example, some of the installed apps can be granted access unintentionally by the users to all of a device's resources to gain, use and share end-users' data. Data in mobile devices and apps, specifically health-critical data in the context of this study, can be leaked to an external host or a third party through excessive app permissions [4, 15], phishing attacks [29], or when installing other mobile apps from unknown resources [54]. Recent studies (e.g., [24, 139]) highlight that end-users have limited security awareness of what they should do to protect their private and health-critical information. Besides, social engineering methods can be used by hackers to deceive end-users into leaking their private information [4, 38]. Molyneaux et al. in [121] indicated that it is difficult for end-users to make security-related decisions when facing security threats. Indeed, most end-users are unaware of such a threat to their data, or are unable to understand the technical mechanisms behind data leakage, which can lead them to ignore the associated security risks. Employing suitable technical solutions, including privacy-preserving mechanisms and two-factor-authentication, cannot address security issues alone; instead, the role of end-users and their understanding of how they should react to different security threats and attacks is an important factor in ensuring the secure use of mobile apps [37].

Technical measures alone may not be enough to ensure security, unless they are complemented with the required human-centric knowledge and practices to protect data [49]. The success factor is significantly influenced by end-users' knowledge and actions [37]. According to a Proofpoint cybersecurity report (2018), 95% of observed attacks exploited the "human factor" rather than relying on software and hardware vulnerabilities (such as phishing emails, or granting unnecessary permissions) [151]. End-users become a threat and can be easily deceived into releasing their health data if they are not fully aware of the security features that they are expected to use [4, 38]. This issue can be seen with technology-based solutions that involve using security features in such a way that users find them difficult to understand [39]. In the view of mHealth apps developers, they consider themselves as having already delivered secure apps by following the principle and practices of secure software development [34]. However, users find these security features hard to understand and use [38]. A recently conducted empirical study (a survey of end-users of mHealth systems) [40] aimed to understand the security knowledge, attitude and behaviour of the end-users. The study defined knowledge as the level of security understanding by the end-users, an attitude refers to how the end-users feel about their knowledge, and behaviour refers to their actions that users perform to ensure security. The results revealed that end-users had the knowledge, attitude about the security measures of the investigated apps. However, end-users' knowledge did not significantly influence their behaviours, indicating that end-users are aware of the risks but are reluctant, or unaware, of appropriate actions that mitigate such security risks (e.g., setting privacy preferences to restrict undesired data access).

To this end, several studies have been conducted that rely on surveys and interviews to collect and analyse end-users' responses based on their security knowledge and behaviour [22, 40, 123-126]. However, the results of such studies could be affected by social desirability (i.e., behaviour does not support the respondents' claims), and/or the sampling method (i.e., relying on a particular group of users). There is a need to empirically measure end-users' actions in a real context. This study aimed at measuring the behaviour of end-users (i.e., users' actions in a specific security scenario based on their knowledge) when dealing with mHealth apps. Clicking on suspicious links, or granting unnecessary permissions when using an app, could allow access to private data within the device. This study aimed to explore and understand the behaviour of end-users of mHealth apps instead of relying on the theoretical phenomenon (i.e., self-reported behaviour via some interviews and questions [22, 40, 123-

126]), which may be attributed to a measurement bias. This study asked the following Research Questions (RQs):

***RQ12**: How do end-users react while facing potential security threats during the usage of mHealth apps?*

The objective of this RQ was to investigate end-users' reactions while facing potential security threats when using mHealth apps.

***RQ13**: What security related mistakes do end-users make while using mHealth apps?*

The objective of this RQ was to identify and analyse various mistakes that end-users make when using mHealth apps.

In order to answer the outlined ***RQs***, we developed an attack simulation app and engaged 105 Android device users to measure their security knowledge. Due to the fact that mHealth apps developed for health purposes can be ranged from general health apps such as decision support health apps to fitness apps for tracking activities and nutrition, we specifically used a fitness monitoring app for our study. We selected the Android platform for our simulation app for two reasons: 1) we know how to develop an Android app, and 2) there were limited resources (i.e., time and funds) to expand the app development to other platforms such as iOS. Participants were exposed to different security attack scenarios, illustrated in the methodology section, and their reactions were recorded. The aim was to assess their security awareness level based on their actions to specific security attack scenarios. Furthermore, through an exit survey, end-users' data (i.e., demographic information) were collected and they were asked to share their thoughts and justify their security decisions. The data analysis for the obtained data consisted of (i) a statistical analysis to measure the reliability and correlations of study items, a descriptive analysis to report the demographic data and our participants' reactions to the security threats, and (ii) a qualitative analysis to present the findings for the open-ended question. The study was performed in a realistic setting and provided empirically-derived usage-driven evidence about the actual behaviour of the end-users of mHealth apps. This study makes the following contributions:

- Simulates most frequently encountered security threats for end-users to investigate the actions and behaviours of end-users. Contrary to existing solutions that rely on survey-based questionnaires, interviews, this solution investigates actions to overcome the potential biased results caused by self-reported behaviours.
- Identifies five main reasons that end-users consider when they face access permissions' requests from a mobile app.
- Provides a fine-grained analysis for end-users who are more vulnerable to security threats/attacks. Such an identification would help to establish guidelines for secure mHealth app usage and improve end-users' security awareness.

This study evaluated end-users security awareness based on empirical evidence and presented interesting insights on how end-users were actually dealing with mHealth apps. The results of this study can benefit

- Researchers to accurately assess the security awareness of end-users, and consider the potential improvements that could be made to the security of mHealth apps.
- mHealth app developers and/ or stakeholders to improve the security knowledge and behaviours of end-users by considering the potential mechanisms, identified in this study, which lead end-users to make improper security decisions.

7.2 Research Method

In this chapter, we used a simulation-based attack, which is detailed in Section 2.4. The results of this chapter are based on 105 end-users who were involved in our study.

7.3 Findings: End-Users' Security Behaviours towards Security Threats (RQ12), and (RQ13)

In this section, we present our findings to answer the ***RQ12***, and ***RQ13*** which we outlined in Section 1.1. We divided our results section into two main sections: (i) Section 7.3.1 which reports the statistical and descriptive analysis, and (ii) Section 7.3.2 provide a thematic analysis for the open-ended question that investigate the reasons for paying attention to the app permissions based on our participants' views.

7.3.1 Statistical and Descriptive Analysis

We enhance our results by including a few statistical analyses, as indicated in Figure 2.6. Such analyses would help to investigate the relationships by relying on the obtained quantitative data. It also helps to determine the significant results within the different demographic data.

7.3.1.1 Measuring the internal consistency of the study items

Cronbach's alpha is used to measure the internal consistency, and how closely related a set of items are as a group [152]. Cronbach's alpha is considered one of the most important and pervasive statistics in research involving test construction and use [153]. The Cronbach's alpha coefficient value should be above 0.70 for a reliable scale [61]. In our study, we consider the permissions request as one focus area and we wanted to determine the reliability of the measurement value. Our analysis indicated that we exceeded the satisfactory level of construct validity and internal consistency (i.e., ≥ 0.7) by having 0.905, which is considered a strong coefficient value [153].

7.3.1.2 Measuring the correlations of the study items

To further assess the relationship between the permissions request items (i.e., strength and direction of the linear relationship), we conducted the Chi-square test to whether there is a statistically significant correlation or not among the obtained data. It also helps to understand the direction of the relationship [62]. Such an investigation can help us to understand when one access permission type changes in value, the other access permission type tends to change in a specific direction. As illustrated in Table 7.1, we found that all the investigated permissions have a positive and statistical significant correlations at 0.01 level. For example, there is a statistically significant correlation between access to device storage and device camera and the chances of observing the obtained correlation (0.792) through random error are less than 0.01. The correlation results ranged from a strong (e.g., 79%: permission to storage and permission to access device camera) to a moderate (e.g., 49%: respond to pop-up window and permission to access device location) relationship. To further elaborate on one example, the correlation indicates that when the score of permission to access storage increases, we expect (i.e., more likely) the score of accessing the device camera to increase positively (it is not a causality relationship). Additionally, our analysis revealed that all the tested items were significantly correlated at 0.01 level.

Table 7.1 Correlation for the Permissions Requests

Permission type	Respond to pop-up window	Permission to storage	Permission to Camera	Permission to contacts	Permission to the audio recording	Permission to location
Respond to a pop-up window	1					
Permission to access device storage	.486**	1				
Permission to access device Camera	.503**	.792**	1			
Permission to access device contacts	.540**	.602**	.770**	1		

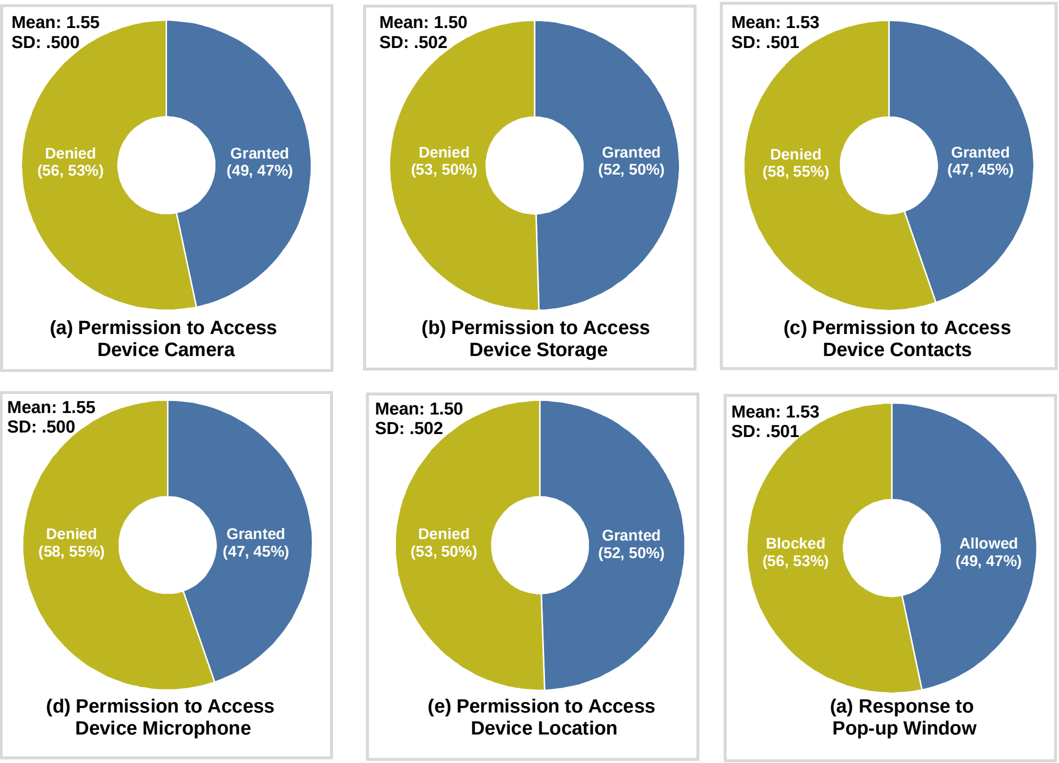
Permission to access device microphone	.502**	.526**	.694**	.730**	1	
Permission to access device location	.486**	.581**	.639**	.641**	.717**	1

**. Correlation is significant at the 0.01 level (2-tailed).

7.3.1.3 Participants reaction to permissions requests

App permissions aim to inform end-users about the resources or features the app is requiring to be functioning. For example, an app that explores the nearby clinics would require access to the device location. Granting access permission is a sign from end-users to allow the app to use the requested resources. The app would be accessing that resources either during usage or while running the background of the app. Depending on the type of the app, access permissions can be divided into normal and dangerous permissions [1]. Granting unnecessary permissions can be classified as dangerous permission that would put the device resources at risk. A malicious script could be hidden into the used APIs that the developer is using without being aware. As a result, exploiting that access permissions to steal private data. Our study investigated participants' decisions when the simulation app requested unrealistic permissions. We requested 630 permissions (i.e., 6 per participant) in the simulation app and we recorded their reactions without reaching the requested resources (including the pop-up window). We found that 296 access permissions (i.e., 47%) were granted to our simulation app, and 334 access permissions (i.e., 53%) were denied. Whilst 33 participants out of 105 (31.4%) had denied all the requested permissions, 77 participants out of 105 (73.3%) had prevented at least one permission, 28 participants out of 105 (26.7%) had responded to grant all the requested permissions for our simulation app.

We further examined our participants' behaviours when they face a phishing link. We presented a pop-up window that offer them free exercises which not available in the app. We found that 47% have granted our request and 53% denied it. Additionally, we requested our participants to grant our simulation app unreasonable permissions to their device software, and hardware, namely, access to the device storage, contacts, camera, microphone, and location. Surprisingly, our findings indicated that 47.5% (± 2.5) of our participants have granted our simulation app access to the requested permissions. Figure 7.1 presents our participants' reactions toward the requested permissions along with the mean and Standard Deviation (SD). Our findings also indicated that granting the app to access the device storage and location was the highest among other permissions (i.e., 50% each).



(a) Permission to Access Device Camera

(b) Permission to Access Device Storage

(c) Permission to Access Device Contacts

(d) Permission to Access Device Microphone

(e) Permission to Access Device Location

(a) Response to Pop-up Window

Figure 7.1 Participants' Reactions to the Requested Access Permissions

7.3.1.4 Relationship between demographic characteristics and participants reactions to access permissions

As indicated in Section 2.4.3 (Phase 3 – Perform Data Analysis), we performed an Independent-Sample T-test for gender since we were comparing two independent populations (i.e., male and female), and a Kruskall-Wallis H test for more than two independent populations (e.g., IT knowledge level, age group, etc.). These statistical tests helped us to determine whether there were statistically significant differences regarding our participants' reactions to the requested access permissions among the defined groups of users, as in Table 7.2. The findings also provide a fine-grained analysis of the security reactions to access permissions for each specific group. For example, which access permissions received the highest allowance by female participants, which group of users are more likely to click on a phishing link, etc. We further investigated the significant differences for the groups whenever applicable (i.e., whenever p-value < .005). We used the Mann Whitney U test to compare the median differences between the overall extents [63, 64]. For each demographic data, we tested the null hypothesis (i.e., *H0: there is no significant difference*) against the alternative hypothesis (i.e., *H1: there is a significant difference*), whereas $\mu1, \mu2, \ldots, \mu k$ refers to population means.

Table 7.2 Variables and Corresponding Codes in SPSS for the Attack-Simulation Study

Simulation app Permissions	Code	Gender	Code	IT Knowledge Level	Code	Age Group	Code	Formal Education	Code
Granted (Allowed)	**1**	*Male*	**1**	*Little or no knowledge*	**1**	*18 – 29 young adult*	**1**	*High school or less*	**1**
								Diploma	**2**
Denied (Blocked)	**2**	*Female*	**2**	*Moderate knowledge*	**2**	*30 – 49 adult*	**2**	*Bachelor degree*	**3**
				Advanced knowledge	**3**	*Above 50 senior*	**3**	*Master's or PhD*	**4**

A. Access Permissions Based on Gender

To understand and compare how male (n=67) and female (n=38) participants reacted to the requested access permissions, we performed a statistical test (i.e., Mann–Whitney U test) to show if there is any significant difference. The overall result indicated that there was no significant difference between male and female (u = 1073.00, z= -1.371, p-value= .170) as in Table 7.3. However, we ran the same test to determine differences in each access permission between males and females. As in Table 7.4, we found that access permission to device storage is statistically significant (u = 915.00, z= -2.757, p-value= .006). The mean rank for females = 62.42 which is higher than the mean rank for males = 47.66 indicating that females have higher attention to granting our simulation app access to the device storage. Thus, we concluded that both males and females in our sample have reacted equally to the requested access permissions excluding accessing device storage.

Table 7.3 Differences in Permissions Requests Based on the Characteristics of Study Respondents

Demography Data Category	Identified groups	N (%)	p-value
Gender	*Male*	67 (64%)	.187
	Female	38 (36%)	
IT Knowledge Level	*Little or no knowledge*	48 (46%)	.001
	Moderate knowledge	42 (40%)	
	Advanced knowledge	15 (14%)	
Age Group	*18 – 29 young adult*	47 (45%)	.001
	30 – 49 adult	53 (50%)	
	Above 50 senior	5 (5%)	
Formal Education	*High school or less*	11 (10%)	.026
	Diploma	14 (13%)	
	Bachelor degree	53 (50%)	
	Master's or PhD	27 (26%)	

Table 7.4 Results for Mann-Whitney U test for Gender Sample

Requested Permission	Respond To Pop-up Window	Storage Permission	Camera Permission	Contacts Permission	Location Permission	Microphone Permission
Mann-Whitney U test	1182.00	915.00	1077.00	1220.00	1177.50	1220.50
Z	-.702	-2.757	-1.512	-.410	-.735	-.410
P value	.483	.006	.130	.682	.462	.682

B. Access Permissions Based on IT Knowledge Level

We conducted a Kruskall-Wallis H test to investigate the significance of granting or denying access permissions based on the participants' IT knowledge (i.e., Little or no knowledge, Moderate knowledge, and Advanced knowledge) as in Table 7.3. Our findings revealed that reacting to access permissions is differed significantly (p=0.001). For the Moderate IT knowledge mean rank = 63.21 which is less than Advanced IT knowledge mean rank = 61.90 and less than Little or no knowledge mean rank = 41.28. Specifically, significant differences were found (using the post-hoc Mann-Whitney U Test) between Little or no knowledge group compared with Moderate knowledge group (p =.001). Whilst we found that there is no statistically significant difference in the security awareness between Moderate knowledge group, and Advanced knowledge group (p=1.000), and there is no statistically significant difference in the security awareness between Little or no knowledge group, and Advanced knowledge group (p=.056). Therefore, we reject H0 and concluded that IT knowledge level had an impact on their decisions to grant or deny access permissions for our participants.

C. Access Permissions Based on Age Group

We conducted the Kruskall-Wallis H test to determine any significant difference among the three age groups (i.e., n=47; young adult, n=53; adult, n=5; senior) regarding how they reacted to the requested access permissions. Our simulation app was developed to help the participants to do exercises as we were advertising for our study. We believe that we were not attracting as many seniors as we should. This could be the main reason that we had a very low number of Senior group (5 out of 105). As in Table 7.3, our findings suggested that there is a statistically significant (p=0.001) when reacting to the requested access permission for the three age groups. Adult group (mean rank = 62.98) were less than Young Adult group (mean rank = 45.49), were less than Senior group (mean rank = 21.30). Whilst we found that there is no statistically significant difference between Senior group and Young Adult group (p= .247), our results revealed that there is a statistically significant difference between Senior group and Adult group (p= .008). We also found that there is a statistically significant difference between Young Adult group and Adult group (p= .010). Therefore, we reject H0: µ1 = µ2 = µ3 and conclude that age did have an impact on the participants when reacting with the requested access permissions.

D. Access Permissions Based on Level of Formal Education

We also wanted to investigate respondents' differences by considering the impact of the level of formal education on our participants. We conducted the Kruskall-Wallis H test on the four groups, which we identified in Table 7.3. Our results indicated that there is evidence (p=0.026) that reacting to requested permissions of those with a postgraduate qualification (mean rank= 60.87) was lower, than those with an education level of Bachelor (mean rank= 56.15), less than those who are having Diploma (mean rank= 40.14), and less than those with High School or less (mean rank= 34.86). We went further to understand the difference within the four levels of education by using the post-hoc Mann-Whitney U test. We found that High school or less group and Bachelor group have a statistically significant difference in granting or denying access permissions (p= .030). We also observed that High school or less group and Postgraduate group have a statistically significant difference (p= .014). Further, we noticed a statistically significant difference between Postgraduate group and Diploma group (p= .034). Our conclusion based on the obtained results suggested to reject H0: µ1 = µ2 = µ3 = µ4. Thus, the level of formal education did have an impact on the participants when dealing with access permissions.

7.3.1.5 Time spent reviewing privacy policy by our participants

App privacy policy is a legal statement that regulates the engagement with end-users. It presents to the end-users how and when their personal data would be collected, retained, or shared with a third party. It also explains what resources the app is requesting, and for what purpose including access permissions, and the financial obligations for the app usage [154]. Some installed apps can do an activity that is risky for the end-user without they being realised [139]. Hence, the privacy policy should be carefully read by end-users before agreeing. In our simulation app and as most mobile apps do, we presented the privacy policy before the installation for our participants, as in Figure 2.8 (a). We aimed to investigate how the participants would react and how much time they spent reading it. To calculate the time, we recorded the time once the privacy policy was presented and the time the participants clicked on the "Continue" button. The average time spent on reviewing the privacy policy for all participants was 8.02 ms to review about 500 words, which requires at least a minute.

Due to the fact that IT knowledge can make a difference in regards to dealing with mobile apps, we further investigated reviewing the privacy policy behaviour of our participants based on their IT knowledge level. Unsurprisingly, we found that participants with advanced IT knowledge (n=15) spent an average time 19.61 ms, as in Table 7.5. While participants with moderate IT knowledge (n=42) spent an average time 7.26 ms, and the participants with little or no knowledge of IT (n=48) spent an average time 5.06 ms. **R96** who spent 5 seconds reviewing the privacy policy wrote "*I don't pay attention to the privacy policy except when the duties and financial responsibility towards the app are mentioned. For example, the policy of cancelling the subscription if the app requires payment or financial fees*".

Table 7.5 Total and Average Time Spent on Reviewing Privacy Policy

Participants Group	Total time spent	Average
All study participants (n=105)	842 seconds	8.02 ms
Participants with little or no IT knowledge (n=48)	243 seconds	5.06 ms
Participants with moderate IT knowledge (n= 42)	305 seconds	7.26 ms
Participants with advanced IT knowledge (n= 15)	294 seconds	19.60 ms

7.3.1.6 Preferred authentication method for our participants

User authentication in our context refers to how the participant wants to log into the simulation app and what method can be used to prove that s/he the legitimate app user. In our previous study [52], we surveyed 101 mHealth apps users to investigate the desired security features they want to be employed. We found that end-users were having different opinions about the authentication method (e.g., employing biometric authentication, interactive authentication, direct access, etc.). Hence, in our simulation app, we provided a variety of options for authentication (ranging from weak, moderate or robust security) to investigate end-users selection. We asked our participants to customize the simulation app by selecting their preferred authentication method. We presented five common authentication methods, namely, none (i.e., without authentication), pattern, Personal Identification Number (PIN), username and password, and Two-factor authentication (2FA). As in Figure 7.2, the majority of our participants (38, 36%) preferred no authentication method. Using Personal Identification Number (PIN) to access the app was selected by 20 participants (i.e., 19%). Using pattern was the preferred option for 13 participants (12%). 23 participants (22%) preferred to have a username and password to log in to the app, and only 11 participants (10%) preferred 2FA.

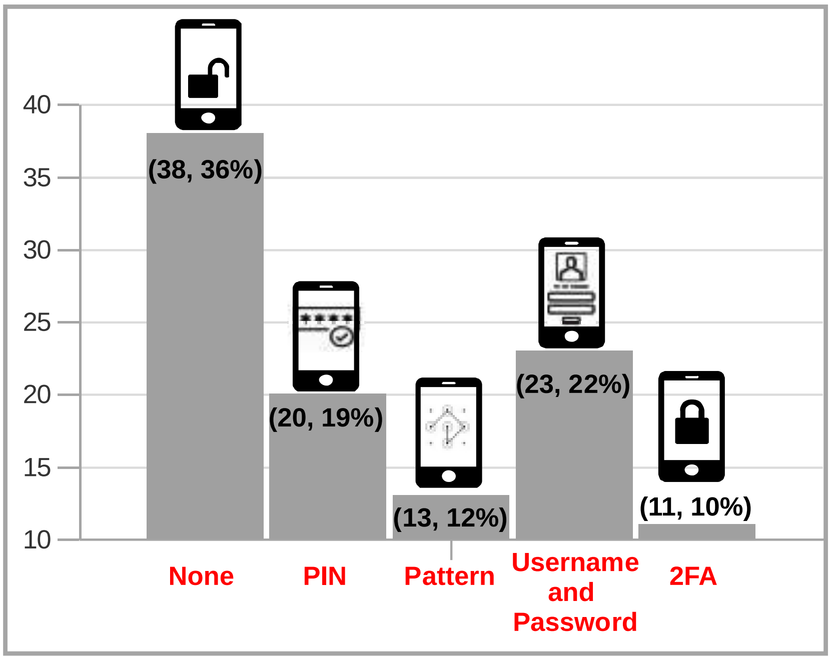


Figure 7.2 Participants Favorable Authentication Method

7.3.1.7 Participants interest in reporting security issues and receiving security advice

In our simulation app, we wanted to investigate the participants' behaviours about reporting security issues within the simulation app in case they noticed. As in Figure 7.3, our findings indicate that only 36 (34%) participants wanted to report security issues and 69 (66%) participants did not want to report any security issues. However, we are unsure whether these participants noticed an issue or not. One possible reason is that participants ignored what they have seen and did not want to bother about these issues. **P97** wrote, *"When I see a security issue with the app, I just uninstall it"*. For further analysis, we looked into the level of IT knowledge of the participants who wanted to report security issue(s) within the simulation app. We found that nine participants with advanced IT knowledge (n=15), 12 participants with moderate IT knowledge (n=42), and 15 participants with little or no IT knowledge (n=48).

We also asked our participants whether they want to receive frequent security advice or not. Our results indicated that 76 (72%) participants accepted getting security advice and 29 (28%) participants refused this idea, as in Figure 7.2. For further analysis, we looked into the level of IT knowledge of the participants who decided not to receive any security advice. Interestingly, the participants were from different levels of IT knowledge. Four participants with advanced IT knowledge (n=15), 13 participants with moderate IT knowledge (n=42), and 12 participants with little or no IT knowledge (n=48).

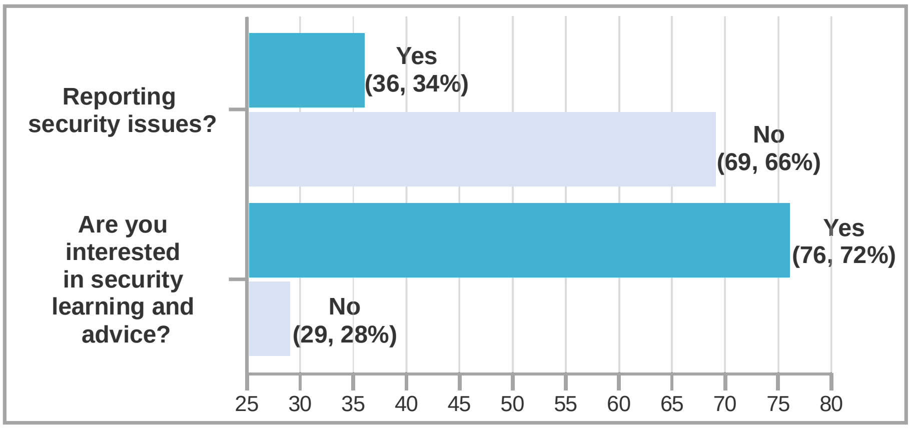


Figure 7.3 Participants Reactions to Reporting Security Issues and their Interest in Security Learning

7.3.2 Reasons for paying attention to the app permissions

In this section, we provide our analysis for the open-ended question that we included in the exit survey, as detailed in Section 2.4.1. We aim to identify the reasons that make our participants pay attention to the requested app permissions based on their views. Based on the obtained responses, we used the qualitative descriptive analysis (Section 2.4.3) to create the conceptualization, as in Figure 7.4. Whilst a few participants perceived the requested permissions positively (Section 7.3.2.1), the majority had negative views about the requested permissions, as in (Section 7.3.2.2– Section 7.3.2.5). Violating/losing privacy were explicitly mentioned by some participants, e.g., **P46**, **P47**, **P51**, **P54**, **P68**, **P82**, **P83**, **P88**, **P89, P92,** and **P98**. Four participants **P42**, **P47**, **P66**, and **P71** indicated that the requestion permissions were unnecessary. **P71** stated, *"[the app] should not access my contacts, photos, or location because the app does not need access to my information"*. We provided cherry-picked examples for each theme to support our findings in Figure 7.4. Each theme is discussed in the following sections.

7.3.2.1 App permissions provide a better usage

The ideal permission for our simulation apps that would make sense to request is accessing fitness data (Health app in iOS). This permission would help to retrieve the data (e.g., steps count, burnt calories, etc.) into our app and perform the required analysis for end-users. However, we did not request this permission purposefully. Instead, we requested permissions to the camera, contacts, microphone, location, photos that would make no logic to be granted. Five participants **P30**, **P45**, **P65**, **P82**, **P87** considered the requested permissions were necessary for the app functionality. The participants assumed that the simulation app was requesting permissions to perform relevant tasks. **P30** mentioned, *"I assume the app needs permissions to help me to have better usage"*, and **P87** wrote, *"It is ok to grant the app to access my location because it is already the case with all other apps"*.

7.3.2.2 Fear of data leakage

Data leakage can be defined as the unauthorised distribution of any confidential or sensitive users data [155]. Whilst app permissions are not the only method for data leakage, providing personal information when registering for the app could potentially be leaked without the app's provider/developer awareness [156]. We are reporting the participants' feedback regarding the reasons for granting or denying app permissions. Our findings revealed that 16 participants **P34**, **P36**, **P46**, **P51**, **P53**, **P54, P65, P68, P71** - **P74, P84**, **P89**, **P92, P98** were having fear of data leakage for either their personal information (e.g., contact number, email address) or device data (e.g., contacts, photos, location). Four participants **P34**, **P51**, **P53,** and **P89** specified that app permissions would permit the app's provider/developer to access their private data. **P89** wrote, *"App permission, based on my knowledge, allow the developer to access my data in the device"*, **P51** stated, *"Giving access to your photos and contacts when it is not necessary can lead to giving the app access of transferring sensitive content to the developers"*, and **P53** indicated *"when I have sensitive data on my phone, [access permissions] my take sms, contacts, or mails to do some things I don't like. "* Four participants, **P51, P68, P72, P92** indicated that they want to protect and maintain their private data. **P51** added, *"…I value my privacy and everything that is on my phone"*, and **P68** wrote, *"To maintain the privacy of my data"*, and **P92** wrote, *"Protecting my personal information and data"*. Three participants **P54**, **P65**, and **P71** mentioned that access permissions would lead to intentionally releasing or making information publicly available to others. **P71** stated, *"The impact can be sharing data publicly such as the app that store the contacts and make it available to others"*, and **P65** wrote, *"Protect my data from being spread out on the internet"*. Five participants indicated giving access permissions can make their private data vulnerable to data leakage. **P84** wrote, *"I pay attention because I have private pictures on my phone and I don't want it to be stolen"*, **P73** wrote, *"It may be leaked my location information and mobile number"*, and **P74** wrote, *"may lose my personal information"*.

7.3.2.3 Fear of their devices being hacked

Access permissions can be the role of attack surface that could be exploited. A compromised app would allow attackers to exploit whatever the app is already connected with including the camera, microphone [157]. Six participants **P42**, **P46**, **P49, P86, P95, P102** expressed their fears of giving more permissions to our simulation app may lead to making their devices insecure. The participants indicated that doing so may make their devices vulnerable to malicious activities such as spying (**P42**, **P46**), or their devices may become hackable (**P49**, **P86**, **P95**, **P102**). Specifically, **R42** stated **"***It will be a back door that will open vulnerabilities to be used to harm the device and its data"*, and **R46** wrote, *"Spy on my data and activity"*. Furthermore, **P86** indicated *"Sometimes permission can be hackable if it not well secured"*, and **P49** mentioned, *"To protect myself from hacks"*.

7.3.2.4 Excessive permission triggers a lack of trust

As indicated in Section 2.4.1, we developed our simulation app and we hosted it on our storage. Since participants had to download from unknown sources, most likely this process gave an impression that our app was suspicious (no reviews or ratings available to view). When we asked our participants the reasons for granting or denying the requested permissions, four participants **P66**, **P73**, **P90,** and **P105** indicated that the simulation app is not trusted to be granted the requested permissions. For example, **P73** stated, *"I will be unhappy about the more permission than needs and don't trust this app using, so that I* *will stop the app from accessing my information"***. R66** found that app permissions should not be requested. **R66** wrote, *"I don't let it go easily. I denied the requested permissions because the app does not need them. Only malicious app would ask for these access privileges."*

7.3.2.5 Fear of using data for objectionable processing purposes

Gathering end-users' data (e.g., contacts, location, etc.) through app permissions can be done easily. However, it becomes a problem in case the app providers share that data without declaration or consent from end-users. This data processing would be objected by end-users if they were asked in advance. Four participants pointed out this concern and indicated that app permissions would gather data to make profits (**P46, P47, P49, R68**). For instance, **P68** stated *"Saving the data and distribute it to private parties. Some companies enable some apps to sell their clients' data*", **P47** wrote *"Transforming users into products, by selling their information"*, and **P49** indicated "*It collects a huge data from the user, and the developer usually sell that data to someone else"*. In addition, two participants reported that the purpose of requesting more permissions is sending advertisements (**P30, P73**). **P73** wrote, "*It may continue to sent my mobile some useless messages latterly*", and **P30** stated "*Sending ads to me*".

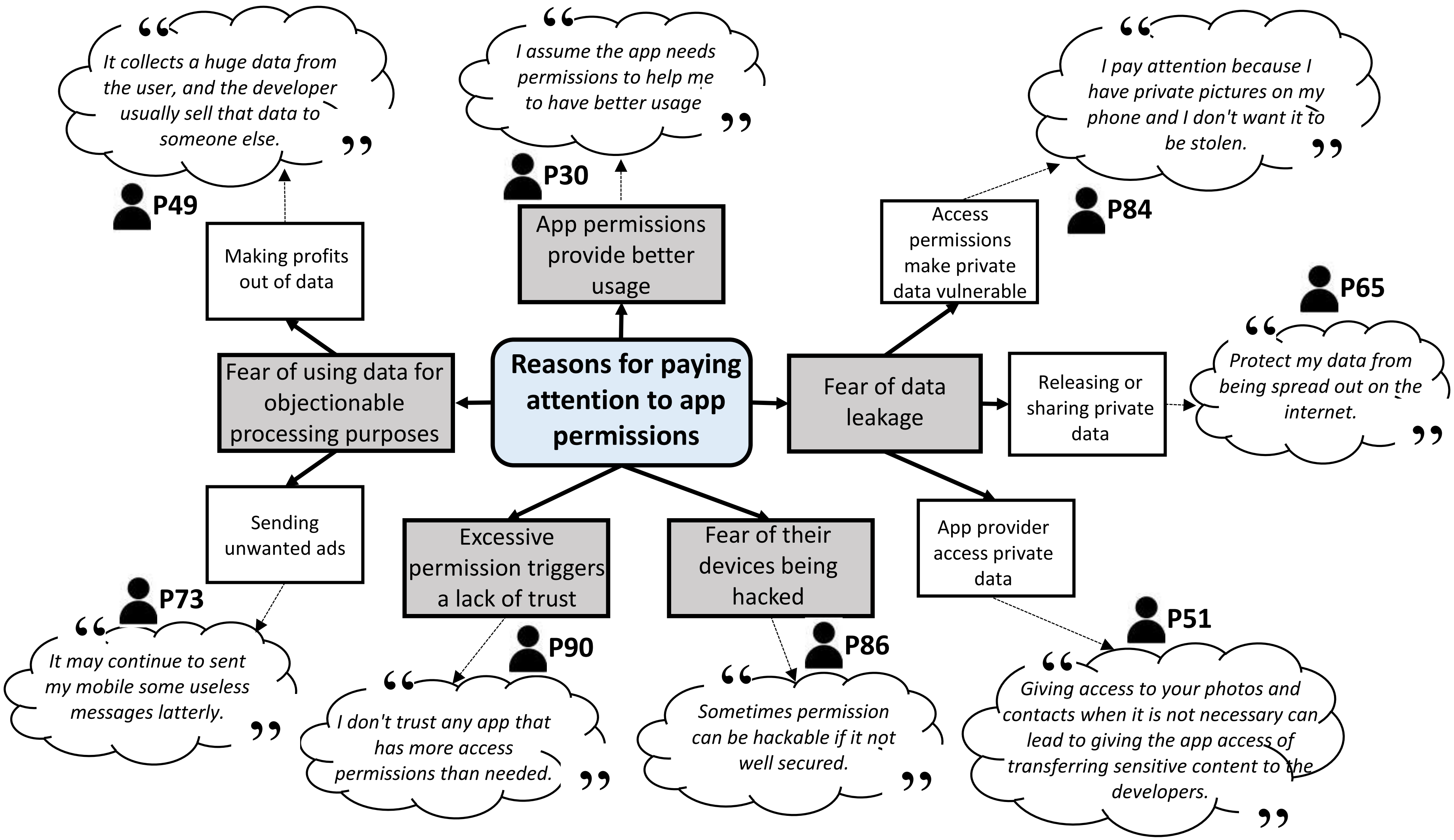

Reasons for paying attention to app permissions
Fear of using data for objectionable processing purposes
Making profits out of data
P49
It collects a huge data from the user, and the developer usually sell that data to someone else.
Sending unwanted ads
P73
It may continue to sent my mobile some useless messages latterly.
App permissions provide better usage
P30
I assume the app needs permissions to help me to have better usage
Excessive permission triggers a lack of trust
P90
I don't trust any app that has more access permissions than needed.
Fear of their devices being hacked
P86
Sometimes permission can be hackable if it not well secured.
Fear of data leakage
Access permissions make private data vulnerable
P84
I pay attention because I have private pictures on my phone and I don't want it to be stolen.
Releasing or sharing private data
P65
Protect my data from being spread out on the internet.
App provider access private data
P51
Giving access to your photos and contacts when it is not necessary can lead to giving the app access of transferring sensitive content to the developers.

Figure 7.4 Participants' Views on the Reasons for Paying Attention to Access Permissions with Some Cherry-Picked Example for Each Theme.

7.4 Discussion

We now discuss the results that highlight the core findings of this study based on the methodological details in Figure 2.6, and outline the potential future work. Table 7.6 guides the discussion and presents a summary of the key findings. The discussion highlights reviewing the privacy policy (Section 7.4.1) followed by discussing the authentication method for the simulation app (Section 7.4.2). We then discuss the results of participants' reactions to requesting access permissions (Section 7.4.3), and finally, the reasons for paying attention to the requested permissions are discussed in Section 7.4.4.

Table 7.6 Taxonomical Classification of the Core Findings for Attack Simulation Approach Study

<table>
<tr><th colspan="7">Measuring the Security Awareness of End-Users about Using mHealth Apps: Attack Simulation Approach</th></tr>
<tr><th>Gender Classification</th><th>Age Group</th><th colspan="2">Formal Education</th><th colspan="2">IT Knowledge Level</th><th>Country</th></tr>
<tr><td>• 64% Male
• 36% Female</td><td>• 45% 18 – 29
• 50% 30 – 49
• 5% above 50</td><td colspan="2">• 10% High school or less
• 13% Diploma
• 50% Bachelor's
• 26% Postgraduate level</td><td colspan="2">• 46% little/no knowledge
• 40% moderate knowledge
• 14% advanced knowledge</td><td>• 39% Saudi Arabia
• 19% Australia
• 18% India
• 10% China
• 14% Others</td></tr>
<tr><td colspan="7">End-users security reactions when facing potential security threats</td></tr>
<tr><th>Reviewing Privacy Policy</th><th>Selecting authentication method for the app</th><th colspan="3">Reactions about requesting access permissions and phishing</th><th>Reporting security issue</th><th>Interest in receiving security learning and advice</th></tr>
<tr><td rowspan="7">• All participants (n=105) spent 14 minutes and 03 seconds.
• Average of 8.02 ms per participant</td><td rowspan="7">• 36% None
• 19% PIN
• 12% Pattern
• 22% Username/ password
• 10% 2FA</td><td>Permission Type</td><td>Granted</td><td>Denied</td><td rowspan="7">• 34% Yes
• 66% No</td><td rowspan="7">• 72% Yes
• 28% No</td></tr>
<tr><td>Pop-up window</td><td>47%</td><td>53%</td></tr>
<tr><td>Device storage</td><td>50%</td><td>50%</td></tr>
<tr><td>Contacts</td><td>47%</td><td>53%</td></tr>
<tr><td>Camera</td><td>45%</td><td>55%</td></tr>
<tr><td>Microphone</td><td>45%</td><td>55%</td></tr>
<tr><td>Location</td><td>50%</td><td>50%</td></tr>
<tr><td colspan="7">Reasons for paying attention to the requested access permissions</td></tr>
<tr><td colspan="7">• App permissions provide a better usage
• Fear of data leakage
- Access permissions make private data vulnerable
- Releasing or sharing private data
- App provider access to private data
• Fear of their devices being hacked
• Excessive permission triggers a lack of trust
• Fear of using data for objectionable processing purposes
- Making profit out of data
- Sending unwanted advertisements</td></tr>
</table>

7.4.1 Reviewing Privacy Policy

Reviewing privacy policy is a vital document that allows apps developers to inform end-users about their data collection practices [114]. Some mobile apps do not provide clear transparency about exactly what data is being shared, with whom, and for what purposes [113]. App developers may share end-users' data with third parties for advertising purposes, or data can be leaked without developers having any thought about how that occurred [158]. The results showed that end-users spent on average 8.02 ms to review the presented privacy policy (about 500 words), which is not adequate to carefully review it, as in Table 7.6. Only nine participants (8%) spent more than 20 seconds reviewing the privacy policy, presented in Figure 2.8 (a). Interestingly, three participants spent rational time reviewing it (i.e., a minute and 55 seconds, a minute and 13 seconds, a minute and 3 seconds, respectively). Most of the participants skipped reading the privacy policy and look for the required action (ticking the box) to install the app. The finding of this is consistent with previous research such as [113, 114, 158]. It should be noted that the entire time that our participants spent on the privacy policy page does not mean that participants were reviewing it. The time was calculated from the time that the privacy policy page loaded until the participants clicked on the continue button. Therefore, future research could consider employing accurate mechanisms such as eye-tracking (which requires accessing the device camera) to record the time that participants are actually spending. Whilst several studies indicated that there is a lack of clarity and transparency in presenting such policies for mHealth apps [1, 113, 114], and recommendations to improve the privacy policy for end-users [12, 15, 16, 19], further work can be done to examine end-users reactions when presenting the privacy policy through using innovative methods including summarizing the main points, using visualization, or a displaying it in the video. This approach would be effective to encourage end-users, especially those who have little or no IT knowledge, to spend more time to understand what data, and how their data are being handled. Exit survey or semi-structured interviews can be considered to allow participants to share their thoughts. Such a study would help to understand how end-users review privacy policy and their understanding of the associated risks of using the apps.

7.4.2 Selecting Authentication Method for the Simulation App

Each type of mobile apps necessities access to the device hardware (e.g., camera, audio recording, etc.) or software (e.g., contacts, images, etc.) to be functioning. Certain apps which deal with sensitive data, require security measures and security awareness from end-users as well. Authentication mechanisms is an important measure that is provided for end-users to provide a layer of protection at the application level. Lack of end-users authentication is considered a serious risk for end-users' data [15]. We aimed to assess our participants' favourable authentication method for the simulation app. We offered them different authentication methods to select from based on their assessment. 67 out of 105 participants (i.e., 63%) believed that our simulation app needs an authentication method, as illustrated in Figure 2.7 and Table 7.6. In contrast, 38 out of 105 participants (36%) selected to access the app without user credentials. We further examined the "none" choice among the different groups of users based on their IT knowledge. We found 18 out of 48 (37%) participants with little or no knowledge of IT selected no authentication. 15 out of 42 (36%) participants with moderate IT knowledge and five out of 15 (33%) participants with advanced IT knowledge selected no authentication. The results indicated that about one-third of each IT level group preferred no authentication for the simulation app. Unlike our findings in Section 7.3.1.4 (b), which indicated that IT knowledge level has a statistically significant difference on app permissions, we concluded that IT knowledge background has no impact on participants' selections for app authentication methods. It is more likely that our participants found that the app is for fitness (based on the study invitation); and hence, the app does not seem to be having sensitive data. Further work needs to consider adopting an app that contains more personal data. This would help to investigate the differences in end-users security reactions in regards to the authentication method. It would be even more insightful to include qualitative data collection (e.g., interviews) to understand the reasons for the participants' selections.

7.4.3 Reactions to Requesting Access Permissions and Phishing

App permissions are designed to ensure that mobile apps access the required resources to work properly [159]. However, requesting access permission beyond the app's purpose of the app is considered malicious access permission. In our simulation app, as in Table 7.6, we requested five permissions to access the participants' hardware/software of their devices to examine their reactions. The requested permissions appeared randomly for the participants at the time of installation and during the runtime of the app. We found that 52 participants (50%) granted the simulation app access to their location. Table 7.7 presents further details about the participants who granted or denied access to their location based on the IT knowledge. **R87** wrote "*It is ok to grant the app to access my location because it is already the case with all other apps*", (a female participant with a bachelor degree, and little or no knowledge of IT). Most likely that end-users have trust in giving some permissions, such as location or specific hardware (e.g., microphone). This could lead to further work to investigate what other access permissions end-users trust, and the reasons that make them trust.

The findings in Section 7.3.1.4 (b) indicated that there was no statistically significant difference for access permissions request based on gender, as in Table 7.3. However, we further found that 53 participants (50%) denied the simulation app access to the storage of their device. Table 7.7 presents further details about the participants who granted or denied access to their device storage based on the IT knowledge. To provide further analysis, we looked into the denied permissions based on gender, as in Table 7.8. We found that females have a higher concern about granting access to their devices. Due to the fact that device storage stores their private photos which cannot be shared, accessing device storage received the highest denial by 26 females (68%). This point confirms our results in Table 7.4 which indicates a statistically significant difference between female and male participants in regards to accessing device storage. Accessing the device location had the lowest denial by 21 females (55%). Furthermore, we found that 53 participants (50%) denied the simulation app access to the storage of their device. **R71** wrote, *"[The app] should not access my contacts, photos, or location because the app does not need access to my information"*, (a female participant with a bachelor degree, and moderate IT knowledge). On the other hand, we found that out of 67 males, 27 (40%) denied access to device storage which is the lowest denial. The highest denial from males was contact and microphone (i.e., 36 males (54%) for each permission request). Table 7.8 presents the numbers of males and females who granted/denied access permissions. **R51** wrote, *"giving access to your photos and contacts when it is not necessary can lead to giving the app access of transferring sensitive content to the developers"*, (a male participant with a bachelor degree, and moderate IT knowledge). In our conclusion, females have a higher concern about requesting access to device storage. Device storage stores their private photos that cannot be shared with others.

Table 7.7 Participants Responses to Requesting Access Permission to their Devices' Locations and Storage based on IT Knowledge Level

Access Permission Type	Options	Little or no IT knowledge (n=48)	Moderate IT knowledge (n=42)	Advanced IT knowledge (n=15)
Access to Location	Granted, 52 (50%)	31 (64%)	16 (38%)	5 (33%)
	Denied, 53 (50%)	17 (36%)	26 (62%)	10 (67%)
Access to Device Storage	Granted, 52 (50%)	29 (60%)	16 (38%)	7 (47%)
	Denied, 53 (50%)	19 (40%)	26 (62%)	8 (53%)

Table 7.8 Participants Responses to all the Requested Access Permission based on Gender

Denied access permissions requests based on gender	Device storage	Camera	Contacts	Microphone	Location	pop-up Window
Female (n=38)	26 (68%)	24 (63%)	22 (58%)	22 (58%)	21 (55%)	22 (58%)
Male (n=67)	27 (40%)	32 (48%)	36 (54%)	36 (54%)	32 (48%)	34 (51%)

7.4.4 Paying Attention to the Requested App Permissions

One of the most common approaches for developers to make a profit out of their apps is embedding an advertising library, which displays ads to the end-users when using the app. Nevertheless, these third party advertisement libraries are granted the same permissions as the developers, and may share or on-sell the information they collect with other entities in the mobile ecosystem [114]. At the same time, mobile apps can be vulnerable to security breaches, especially when the app is developed through poor security practices [34]. The simulation app which the study used requested access to device resources (six types of resources as presented in Section 7.3.1.3, and Table 7.6). The simulation app purposefully lacks transparency (i.e., no clarifications on why these permissions were requested) to examine and record the participants' reactions. All requested permissions popped up to the participants soon after the app installation or when they were using the app. Almost 50% of our participants granted the simulation app permissions. Interestingly, a few participants claimed that they paid attention to app permissions because they were worried about their privacy. However, we found a contradiction with their responses in the exit survey. For example, **R34**, and **R73** (both are males with moderate IT knowledge) fully granted our simulation app the requested permissions. **R34** wrote, "*To not get permissions to private images*", and **R73** wrote, "*I will be unhappy about the more permission than needs and don't trust this app using, so that I will stop the app from accessing my information*". The results also indicated that end-users can easily fall into the ambush of sharing their data and devices. This triggers the alarm that end-users need to pay careful attention when installing and using mobile apps. Further work can be done using a similar approach by allowing the participants to share their views about granting or denying permissions after every single request. In addition, a summary report can be shared with each participant as soon as s/he completes the study. Such a summary should explain what mistakes the participant has done with their potential impacts, and what could have been done better when facing these access permissions. Consequently, this would help to increase the security awareness of the end-users before thinking to grant any app permission.

7.5 Related Work

We now position the work reported in this chapter with respect to related studies.

As discussed in Section 3.3.2, previous studies used two methods to measure the security awareness of the end-users of mobile apps. The most common approach is assessing the security awareness through questionnaires (i.e., surveys, interviews, focus groups, etc.). In this approach, researchers, such as in [22, 40, 123-126], request the participants to answer self-report questions about what security-related actions they took in the past, or intend to take in the future [122]. However, the self-reported behaviour approach could be resulting unreliable findings in some cases [54]. The second approach is measuring security awareness using objective data sources such as [54-59]. This approach tends to measure the behaviour by installing an agent and allows the researcher to monitor the participants' reactions to a specific security phenomenon.

A recently published work in 2020 by Aljedaani et al. [40] surveyed 101 participants to measure the security awareness of end-users about using clinical mHealth apps. The study utilised the Human Aspects of Information Security (HAIS) model to measure end-users' security knowledge, attitude, and behaviour. The results revealed that end-users had the knowledge, attitude about the security measures of the investigated apps. However, end-users' knowledge has not significantly influenced their behaviours. Besides the potential bias in data collection (i.e., self-reported behaviour), the study participants were from two health providers in one region. The study by Zeybek et al. in 2019 [124] surveyed 120 participants in a public institution to investigate mobile apps users' security habits (i.e., installation and rejection for app's permissions, the usage of antivirus app, locking screen, frequent updates for the apps, and installation for the apps from official store). The study concluded that awareness training and malware analysis through internal experts or external institutions are required. The results can be biased due to the fact that employees might report their best behaviour as they have been informed that the study outcomes might be view by their senior managers. Watson et al. [125] surveyed 94 participants and Mylonas et al. [22] surveyed 458 participants to investigate the security awareness of mobile devices users about critical security options (i.e., device settings, user behaviours). While the findings of Watson et al. revealed that participants, especially those without strong IT knowledge, tend to ignore or be unaware of many critical security options, Mylonas et al. found that users were not adequately prepared to make appropriate security decisions. Further, users had poor adoption of 'pre-installed' security controls, such as encryption, remote data wipe, and remote device locator. The limitations that could affect the results can be relying solely on the self-reported behaviour, and focusing on a specific group of participants (age 15 – 30).

Producing inaccurate results is one of the limitations of survey-based due to the self-reported behaviour. Thus, studies developed more effective mechanism to measure security awareness by measuring the actual behaviour of end-users, namely a simulation-based approach. Furthermore, studies were found involving other methods, (e.g., interviews, think aloud, exit survey) to allow participants to share their thoughts instead of relying on a simulation-based approach only. To indicate some relevant studies, Wijesekera et al. [59] conducted an experiment with 36 participants to examine users' ability to deny applications access to protected resources. Felt et al. [57] evaluated whether or not Android users pay attention to, understand, and act on permission information during installation. The study was conducted through two usability studies: an Internet survey of 308 Android users, and a laboratory study wherein 25 participants were interviewed and observed. Bitton et al. [54] measured the security awareness of smartphone users (i.e., 162 participants) for specific attack classes. The actual behaviour was measured using a developed mobile agent and network traffic monitor and compared the findings with self-reported behaviour, which have been collected through a survey. Barth et al. [55] examined the privacy paradox by focusing on the actual behaviour and eliminating the effects of a lack of technical knowledge, privacy awareness, and financial resources. The study was conducted as an experiment (including a questionnaire) on the downloading and usage of a mobile phone app among 66 Computer science students by giving them sufficient money to buy a paid-for app.

Security characteristics (Section 2.4.1, Table 2.1) in this study were carefully selected based on the existing research. This study selected reviewing privacy policy because it is an essential part of any mobile apps to outline the end-users rights. Steinfeld in 2016 [160] conducted a study to understand how end-users read the online privacy policy. The study findings indicated that when a presenting privacy policy by default, participants tend to read it very carefully, whereas when given the option to sign their agreement without reading the policy, most participants skip reviewing the policy. The study also found that participants who actively choose to read the policy spend significantly less time and effort on reading it than participants in the default condition. Customizing the app based on the preferred authentication came after the installation. This study took the findings in Chapter 6 into consideration. End-users had different views in regards to authentication mechanism; and hence, the study provided five different authentication mechanisms, as in Figure 7.2 to investigate the preferable method to access the simulation app. The study showed the access permissions requests randomly during using the app to help participants understand the purpose of the requested permissions. The study by Felt et al. [161] indicated that end-users may be able to understand why such a permission request is needed if some of these requests are granted during runtime consent dialogues, rather than Android's previous install time notification approach. Granting or denying permissions at the runtime would make more sense for end-users in providing additional contextual information. Denying the permission would lead to blocking the app from doing the task that is supposed to be done. As a result, end-users will understand based on what they were doing at the time that resources are requested, and have a better idea of why those resources are being requested [59]. Hence, the study selected the requested permissions because end-users can see them as normal requests.

Studies including [22, 40, 123-126] measured the security awareness of end-users about using mHealth apps. However, all the indicated studies were measuring security behaviour through a questionnaire, which is not sufficient to report accurate measurement. Other studies including [54-59] tended to measure security awareness using action-based research that can provide better results. However, none of the action-based research studies was focused on mHealth apps. To the best of our knowledge, there has been no experimental research study to measure end-users security awareness when using mHealth apps. We investigated the security awareness of end-users of mHealth apps via an attack simulation approach. We measured end-users reactions by posing a few security threats, and monitor their spontaneous reactions. Furthermore, the presented study in this chapter relied on multiple data sources (i.e., simulation-based, and exit survey), used mHealth app as a simulation app, and engaged end-users with diverse backgrounds, namely, age, gender, education level, IT knowledge level, and geographical distribution.

7.6 Conclusions

The use of mobile computing has offered a multitude of context-aware services, ranging from social networking to fitness monitoring and smart healthcare [1]. According to a recent report, 'The Mobile Economy 2020', published by GSMA, approximately 67% of the global population subscribed to mobile services by the end of 2019 with an expected increase to 70% by 2025 [2]. The increased popularity of mobile apps usage is on a raise every year. These apps collect, store, and transmit users' data that can be sensitive depending on the type of mobile app. Security has become an essential attribute that has to be considered. The role of end-users is also essential to mitigate any security risks. In this study, we conducted a user study to measure the security awareness towards using mHealth app. We developed a simulation app and involved 105 participants who installed the app and completed the study (i.e., reacting to all tasks, and filling out the exit survey). We enhanced our data collection by the demography data of the respondents, which helped us to highlight the supporting factors such as age group, educational background, and the level of IT knowledge that increase the participant's security awareness. The key findings of our study are:

- The privacy policy is overlooked. The average time spent on reviewing it was 8.02 ms. More time should be given to review the legal obligations of the app are.
- 36% of our participants selected no security method for the simulation app as their favourite method to access the app.
- 47.5% (± 2.5) of our participants have granted our simulation app access to unnecessary permissions (e.g., accessing contacts, camera, location, etc.).
- Privacy is the main driving force to pay attention to the requested permissions.

This study examined end-users' security awareness through an attack simulation approach, and it has uncovered some possible directions for future work:
(i) It could be further extended to include a larger number of participants with different demographic information. Future studies could also include other security threats which have not been covered in this study (such as the strength of passwords, changing passwords, data security at rest and data in transit, etc.).
(ii) It could be further extended by using the same approach but by also providing a summary report to be shared with each participant as soon as s/he completes the study. Such a summary could explain what mistakes the participant has made and the potential impacts of those mistakes, and what could have been done better when facing these access permissions.

Chapter 8

Conclusions and Future Works

Due to the proliferation of mobile devices and their offered capabilities, and their potential to revolutionise how healthcare services are delivered, mobile health (mHealth) Applications (apps) have recently begun to gain more attention. Nevertheless, security remains an issue. In this thesis, three empirical studies on the security of mHealth apps are presented. The main goal was to understand the security views (of app developers and end-users) and security reactions (of end-users). To that end, a systematic literature review (developers' views) was conducted first to establish a solid background understanding of existing studies. Followed by an ad-hoc literature review which was undertaken to understand end-users' views and reactions when utilising mHealth apps. Secondly, 97 mHealth apps developers were surveyed to understand the security challenges and practices as well as motivational factors, to ensure the security of mHealth apps. Thirdly, a study with 101 end-users, who use mHealth apps in the clinical setting, was conducted to understand their knowledge, attitude, and behaviour towards using mHealth apps, as well as understand how these factors influence the security of mHealth apps. Further, the study investigated the security issues they experience, security preferences that would make them feel more comfortable when using mHealth apps, and the employed methods that have helped them to become aware of the security of mHealth apps. Finally, a use case study with 105 end-users was conducted to understand their security behaviour when they encounter certain security threats. In this chapter, the findings are summarized for the research questions introduced in Chapter 1, and then suggest some promising areas for future work.

8.1 Findings and Contributions

We now summarize the key findings of this thesis with respect to the research questions outlined in Chapter 1.

8.1.1 Developers' views of security of mHealth apps

A. Through conducting a systematic literature review reported in Section 3.1, we identified nine challenges that hinder the developers of mHealth apps from developing secure apps. These challenges are 1) lack of security guidelines and regulations for developing secure mHealth apps, 2) developers' lack of knowledge and expertise in secure mHealth app development, 3) lack of stakeholders' involvement during mHealth app development, 4) no/little developers' attention to the security of mHealth app, 5) lack of resources for developing secure mHealth apps, 6) project constraints during the mHealth app development process, 7) lack of security testing during mHealth app development, 8) developers' lack of motivations and ethical considerations, and 9) lack of security experts' engagement during mHealth app development.

B. Through an empirical study with 97 mHealth apps developers, Chapter 4, we identified ten challenges that developers face with respect to implementing security. The identified challenges are 1) insufficient security knowledge of the developers, 2) little or no budget for employing security, 3) lack of involvement of security experts during software development, 4) poor security decisions during the development process, 5) assumptions about security issues resolved by app testers, 6) project constraints which compromise the security, 7) lack of security testing, 8) the assumption that users are not very interested in security, 9) dealing with legal obligations, policies and procedures, and 10) the challenges of maintaining mHealth app and data. Furthermore, we propose a taxonomy for the security practices that mHealth apps developers follow to incorporate security measures during the development of mHealth apps, as in Figure 4.2, Chapter 4. We analysed the security practices based on the Microsoft secure software development process which involves five development tasks, namely, Requirements Engineering, Software Design, Software Implementation, Software Verification, and Software Deployment. The taxonomy helped with conceptualization and quick identification of all the practices that developers perceive as effective in enabling or enhancing app security. Moreover, we identified the motivational factors that lead to developers developing secure mHealth apps. These motivational factors are 1) having a security leader in the team overseeing the development of secure mHealth apps, 2) knowing that secure development maintains the vision and reputation of the organisation, 3) knowing that insecure mHealth apps have consequences, 4) having previous experience of app failure, 5) realising that secure app development can lead to career opportunities and promotion, 6) realising that secure app development can bring reward and recognition, 7) the existence of organisational practices for ensuring security, 8) the desire to fulfil ethical obligations, 9) the desire to fulfil legal obligations, and 10) the desire to fulfil reduce the cost of maintaining the app.

8.1.2 End-users' security knowledge and perception of mHealth apps

A. Through conducting an ad-hoc literature review in Section 3.3, we identified the security perceptions of end-users when using mHealth apps. We have found that end-users' perceptions of security when using mHealth apps can vary based on the type and context of data that is handled by the apps, the time and context of access, i.e., who accesses the data, when, and for what reasons. Furthermore, we report the security issues that end-users of mHealth apps are concerned about, and the security measures that increase end-users' confidence level when using mHealth apps including enabling end-users to adjust security settings, enforcing regular updates for passwords, and allowing the monitoring of data access via access logs, using biometric verification, and allowing end-users to wipe the device remotely if the device is lost or stolen. Table 3.4 presents a summary of the existing studies and position the work presented in Chapter 5, and Chapter 6.

B. Through a collaboration with two mHealth providers in Saudi Arabia, we conducted a survey questionnaire with 101 end-users, who use mHealth apps in the clinical setting. We aimed to understand the security perception of end-users about using mHealth apps that contain health-critical data.

- In Chapter 5, we determine the level of security knowledge, attitude and behaviour of mHealth apps end-users towards using mHealth apps, as in Table 5.5. In addition, we performed statistical analysis (Linear regression analysis) to understand the relationships between security knowledge, attitude and behaviour, and how these factors influence end-users of mHealth apps. The results suggest that end-users' security-specific knowledge:

  - Strongly influences their attitude towards the security of mHealth apps. This means that end-users are aware of the risks (e.g., of their critical health data being stolen or tampered with) and like to mitigate them (e.g., by using app support for data encryption).

  - Does not significantly influence their behaviour. This means that end-users are aware of the risks (e.g., of their private data being shared with third parties for targeted ads) but are reluctant or unaware of appropriate actions that mitigate risks (e.g., setting privacy preferences to restrict undesired data access).

- In Chapter 6, we disclose the importance of securing health-critical data within mHealth apps based on end-users' views. The vast majority of the surveyed end-users (95%) were concerned about securing their health-critical data. Our findings also reveal that majority of the end-users were unaware of the existing security features provided (e.g., restricted app permissions). We reported the desired security features for mHealth apps: usable security for authentication (e.g., biometric authentication) and privacy preservation for health data (e.g., protection of health data from unauthorised access). End-users suggested that protocols such as two-factor authentication positively impact security but compromise usability. Security awareness via peer guidance, or training from app providers can increase end-users' trust in mHealth apps.

8.1.3 End-users' security behaviours towards using mHealth apps

A. Through conducting an ad-hoc literature review in Chapter 3, we identified the methods used to measure the security awareness of the end-users of mobile apps. We found that it was possible to measure the security awareness of the end-users through questionnaire-based studies, and simulation-based approaches. As in Table 3.5, we summarize the findings of existing studies and provide a comparative analysis that helped to understand and conduct the study into end-users security behaviour.

B. Through conducting an experimental study with 105 Android users, Chapter 7, we provide empirical evidence about the actual behaviour of end-users of mHealth apps when they face security threats/attacks. Our findings indicate that end-users did not spend sufficient time reviewing the provided privacy policy (average time spent is 8.02 ms). Opening the app without an authentication method is the preferable option for 36% of our participants, and using 2FA is the least preferable authentication method for 11% of the participants. 47.5% (± 2.5) of our participants granted/allowed our simulation app access to the six types of the requested permissions (e.g., contacts, camera, location, etc.). Only 34% had the intent to report security issues they noticed in our simulation app, and 28% were not interested in receiving security advice. Whilst there was no statistically significant difference between the genders (p= .187) of our participants when they reacted with the requested permissions, we found that the level of IT knowledge, age, and level of education were statistically significant (p= .001, p= .001, and p= .026 respectively). Our participants were mainly concerned about their privacy (e.g., fear of data leakage, fear of their devices being hacked, and fear of using data for objectionable processing purposes, etc.) when we asked them about the reasons for paying attention to the app permissions. We concluded that these factors had an impact on our participants' selections to grant or deny the permissions.

8.2 Opportunities for Future Research

The studies presented in this thesis make a significant contribution to the understanding of the security of mHealth apps based on developers' perspectives and end-users' perspectives. However, we believe there are still open areas that can be further investigated particularly in regard to the security of mobile apps or mHealth apps. Hereafter, we discuss potential future research directions.

8.2.1 Evaluating the Security Practices of Developing Secure mHealth apps

We conducted our study (presented in Chapter 4, Section 4.4.2) to investigate the security practices to ensure the development of secure mHealth apps. We present a taxonomy of the development practices of our respondents, as in Figure 4.2, and how they ensure security throughout the SDLC. Thus, we propose empirical validation of the security practices and investigate the approaches that lead to the selection of these practices (e.g., previous experience, having a security leader, etc.), for which type of mHealth app(s) these security practices are followed, what obstacles and constraints that the development team face, and what the obtained benefits are (e.g., ease of use). It should be noted that ensuring security is a process that needs to be incorporated during all SDLC phases (i.e., Security by Design approach); it also would be worth investigating the effectiveness of combining several security practices at the single phase or throughout the development process. This would help to compare the best practices and the followed practices to achieve security by mHealth app development teams. Moreover, since mHealth app development organisations play an essential role in ensuring the security of the apps, more work is needed to investigate what sort of support mHealth app developers are getting from their organisations, how the given support helps to prioritize security, and ensure the development of secure mHealth apps.

8.2.2 Conducting a Security Analysis for mHealth Apps

Due to the fact that mHealth apps capture and handle personal data (such as age, gender, location) and health-critical information (such as medical history, and disease symptoms) which can be vulnerable to various security threats, an in-depth security analysis of these apps is much needed to understand the current security status. This process would help to bridge the gaps, and help relevant entities (e.g., stakeholders, health providers, policy makers, researchers, developers) to tackle security issues within mHealth apps. We propose analysing the most downloaded mHealth apps from the app stores. mHealth apps for medical purposes can be potential targets since they record and monitor critical health data; hence we recommend excluding the fitness apps category. Rigorous security testing could be performed through static and dynamic analysis based on predefined assessment criteria (e.g., privacy issues, secure communication issues, cryptographic issues, etc.). Such an analysis would require the adoption of mature tools for each security issue to scan the selected mHealth apps and identify the existing vulnerabilities. To avoid any legal issues, researchers should communicate with the apps providers to inform them about their intention. Furthermore, the results of the security analysis would need to be reported to the apps providers with recommendations.

8.2.3 Investigating End-Users Security Awareness about Using other Mobile Apps

Mobile apps have become an essential part of end-users daily activities. Not only mHealth apps, but also other apps (such as mobile banking apps, shopping, and commercial apps) handle confidential personal information that needs to be secured. Some of this information would be valuable for attackers to even control the apps (e.g., username, PIN code, email address, contact number, etc.). Therefore, further investigation should be conducted to understand end-users' security awareness about using mobile apps from another domain. Such an understanding would help to provide a fine-grained analysis of security and usability based on end-users' views. The findings could be compared with the end-users' views that we presented in Chapter 5, and Chapter 6. It would also be helpful to understand the role of app providers in supporting end-users to become aware of secure app use. End-users, especially those with little or no knowledge of IT, need to be educated to identify common security threats. For example, end-users can be tricked by mobile malware which represents a risk when it is granted access to the devices' resources (e.g., sensitive data may be transferred to a third party). The outcomes of this investigation would provide new information to end-users, and hence improve their security awareness when using mobile apps.

8.2.4 Measuring the Security Behaviour by Targeting a Specific population

We selected the participants for the experimental study (Chapter 7) randomly. Based on the demographic data for our participants, we had a low number for some specific groups (e.g., above the age of 50, female). In fact, it was challenging to convince particular participants to participate because the simulation app (Workout app) that we used was not of interest to them. Thus, future work may consider targeting specific cultural and demographic groups to compare the new results with our findings. Another avenue of research could involve developing a simulation app that helps to easily collect the required data using different mobile OS platforms. Recruiting participants for an attack simulation approach study could be challenging; thus, providing incentives for participants would boost data collection and response rates. Further research needs to consider the end-users who have little IT knowledge since they are more vulnerable to security threats/attacks. Advice could be provided whenever the users make a decision that has security risks or could lead to security risks. We believe this approach would help educate end-users and increase their security awareness. It would also enable early identification for end-users whenever they are vulnerable to a security threat.

8.2.5 Initiatives to Increase the Security Awareness of End-Users of mHealth Apps

Whilst mHealth apps can play a game-changer role in fighting diseases and preventing the outbreak (e.g., COVID-19 pandemic, or another epidemic such as Dengue), these apps can be exploited by attackers to target end-users with malicious activities. Developing a security awareness program to help end-users to understand the potential security threats and take proper security decisions is an important step to consider. Therefore, we propose a few initiatives to increase the security awareness of end-users of mHealth apps, which could create an opportunity for further research. First, training programs and campaigns by the health providers would be helpful to influence the security behaviour of end-users and recognise the potential security threats. A second method would be to apply a game-based learning approach. This approach would couple mHealth apps with gaming technology that would help to simulate real-world situations. For example, end-users could be challenged to detect malicious activities when using mHealth apps, or managing access permissions required by mHealth apps. A third option could be to establish a portal that guides end-users virtually to empower their knowledge about a variety of mobile threats that might put end-users' data at risk. It would be even better to conduct a frequent assessment to ensure the effectiveness of the employed method in raising security awareness.

Appendix A

Selected Studies in the Systematic Literature Review

ID	Author(s)	Title	Venue	Pub. Year
S1	S. Gejibo, F. Mancini, K. A. Mughal, R. A. B. Valvik, and J. Klungsøyr	Secure data storage for mobile data collection systems	International Conference on Management of Emergent Digital EcoSystems	2012
S2	D. D. Luxton, R. A. Kayl, and M. C. Mishkind	MHealth data security: The need for HIPAA-compliant standardization	Telemedicine and e-Health	2012
S3	R. Adhikari, D. Richards, and K. Scott,	Security and privacy issues related to the use of mobile health apps	25th Australasian Conference on Information Systems	2014
S4	D. He, M. Naveed, C. A. Gunter, and K. Nahrstedt	Security Concerns in Android mHealth Apps	Annual Symposium proceedings / AMIA Symposium.	2014
S5	T. L. Lewis and J. C. Wyatt	mHealth and mobile medical apps: a framework to assess risk and promote safer use	Journal of medical Internet research	2014
S6	S. Becker, T. Miron-Shatz, N. Schumacher, J. Krocza, C. Diamantidis, and U.-V. Albrecht	mHealth 2.0: experiences, possibilities, and perspectives	JMIR mHealth and uHealth	2014
S7	I. Mergel	The Long Way From Government Open Data to Mobile Health Apps: Overcoming Institutional Barriers in the US Federal Government	JMIR mHealth and uHealth	2014
S8	S. Arora, J. Yttri, and W. Nilsen	Privacy and security in mobile health (mHealth) research	PubMed, Alcohol Research	2014
S9	Y. Cifuentes, L. Beltrán, and L. Ramírez	Analysis of Security Vulnerabilities for Mobile Health Applications	The Seventh International Conference on Mobile Computing and Networking	2015
S10	A. Carter, J. Liddle, W. Hall, and H. Chenery	Mobile phones in research and treatment: ethical guidelines and future directions	JMIR mHealth and uHealth	2015
S11	K. Knorr and D. Aspinall	Security testing for Android mHealth apps	IEEE 8th International Conference on Software Testing, Verification and Validation Workshops,	2015
S12	F. Zubaydi, A. Saleh, F. Aloul, and A. Sagahyroon	Security of mobile health (mHealth) systems	IEEE 15th International Conference on Bioinformatics and Bioengineering	2015
S13	A. Landman, S. Emani, N. Carlile, I. D. Rosenthal, S. Semakov, J. D. Pallin	A Mobile App for Securely Capturing and Transferring Clinical Images to the Electronic Health Record: Description and Preliminary Usability Study	JMIR mHealth and uHealth	2015
S14	T. Dehling, F. Gao, S. Schneider, and A. Sunyaev	Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android	JMIR mHealth and uHealth	2015

ID	Author(s)	Title	Venue	Pub. Year
S15	J. Hsu, D. Liu, Y. M. Yu, H. T. Zhao, Z. R. Chen, J. Li	The top Chinese mobile health apps: A systematic investigation	Journal of Medical Internet Research	2016
S16	D. Kotz, C. A. Gunter, S. Kumar, and J. P. Weiner	Privacy and Security in Mobile Health: A Research Agenda,"	Computer, vol. 49, pp. 22-30	2016
S17	M. Zens, N. P. Sï¿½dkamp, and P. Niemeyer	Back on track: cruciate ligament study via smartphone: Practical example of possibilities for the Apple ResearchKit	Arthroskopie, vol. 29	2016
S18	G. Thamilarasu and C. Lakin	A security framework for mobile health applications	5th International Conference on Future Internet of Things and Cloud Workshops	2017
S19	J. Müthing, T. Jäschke, and M. C. Friedrich	Client-Focused Security Assessment of mHealth Apps and Recommended Practices to Prevent or Mitigate Transport Security Issues	JMIR mHealth and uHealth	2017
S20	M. Bradway, C. Carrion, B. Vallespin, O. Saadatfard, E. Puigdomènech, M. Espallargues	mHealth Assessment: Conceptualization of a Global Framework	JMIR mHealth and uHealth	2017
S21	T. Mabo, B. Swar, and S. Aghili	A vulnerability study of Mhealth chronic disease management (CDM) applications (apps)	Advances in Intelligent Systems and Computing	2018
S22	A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, and C. Patsakis,	Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice	IEEE Access	2018
S23	M. Hussain, A. A. Zaidan, B. B. Zidan, S. Iqbal, M. M. Ahmed, O. S. Albahri, et al.	Conceptual framework for the security of mobile health applications on Android platform	Telematics and Informatics	2018
S24	L. Hutton, B. A. Price, R. Kelly, C. McCormick, A. K. Bandara, T. Hatzakis, et al.	Assessing the privacy of mhealth apps for self-tracking: heuristic evaluation approach	JMIR mHealth and uHealth	2018
S25	M. Aliasgari, M. Black, and N. Yadav	Security vulnerabilities in mobile health applications	IEEE Conference on Application, Information and Network Security	2019
S26	Y. M. Al-Sharo	Networking issues for security and privacy in mobile health apps	International Journal of Advanced Computer Science and Applications	2019
S27	L. Parker, V. Halter, T. Karliychuk, and Q. Grundy	How private is your mental health app data? An empirical study of mental health app privacy policies and practices	International Journal of Law and Psychiatry	2019
S28	M. Srivastava and G. Thamilarasu	MSF: A comprehensive security framework for mhealth applications	International Conference on Future Internet of Things and Cloud Workshops	2019
S29	T. Wykes and S. Schueller	Why reviewing apps is not enough: Transparency for trust (T4T) principles of responsible health app marketplaces	Journal of Medical Internet Research	2019
S30	T. Wykes, J. Lipshitz, and S. M. Schueller	Towards the Design of Ethical Standards Related to Digital Mental Health and all Its Applications	Current Treatment Options in Psychiatry	2019
S31	J. Muchagata, S. Teles, P. Vieira-Marques, D. Abrantes, and A. Ferreira	Dementia and mHealth: On the Way to GDPR Compliance	Communications in Computer and Information Science	2020
S32	B. Aljedaani, A. Ahmad, M. Zahedi and M. Ali Babar	An Empirical Study on Developing Secure Mobile Health Apps: The Developers' Perspective	Asia-Pacific Software Engineering Conference	2020

Appendix B

Survey Instrument for Developers' Study

Research Title: An Empirical Study on Developing Secure Mobile Health Apps: The Developers Perspective

Ethics approval: H-2019-115

The University of Adelaide, Australia

General Information

Whilst mobile health applications (apps) hold great promises to improve and facilitate healthcare domain. However, the security can be a challenging task to achieve by mHealth apps developers'. Health data can be disclosed or modified to lead to serious impact (e.g., medical identity theft). Thus, there is a high demand to secure mHealth apps to prevent data breaches and data misuse. This issue can resolved earlier during the development of mobile health apps by ensuring that all security aspects have been well addressed by apps developers'. This research aim is aimed at understanding and addressing the challenges that influence developing secure mobile health apps. Furthermore, this research would help to understand the security practices for developing secure mobile health apps, and the developers' motivational factors to ensure the security. This study will be conducted through a survey to allow us collect qualitative and quantitative data that can be beneficial for the research.

Who do I contact if I have questions about the project?

Any questions regarding the project and survey can be asked via:

Bakheet Aljedaani, Bakheet.aljedaani@adelaide.edu.au
Prof. Muhammad Ali Babar, ali.babr@adelaide.edu.au
Dr. Christoph Treude, Christoph.treude@adelaide.edu.au

Why am I being invited to participate?

You are being invited as you are a developer for mobile health apps to participate in our study. You should be over 18 years of age and have published at least one mobile health app or currently working on developing one. You should be able to communicate in English to involve in this study.

What am I being invited to do?

You are being invited to participate in an online survey about the security challenges you and your respective organisation might experience when developing mobile Health apps, and what strategies you considered to address those challenges. The survey contains three main sections including general questions (e.g., your role, your experience, etc.), developers' security knowledge, and the supporting factors for developing secure mobile health apps. The survey questions have been formulated in different forms (i.e., multiple choice questions, Likert questions and open-ended questions) to allow you to share with us your development experience.

If you are interested to receive the results of the survey when published, you can provide your email address at the end of the survey.

How much time will my involvement in the project take?

Answering the online survey will take approximately 15 minutes of your time. But it can take shorter or longer time.

Are there any risks associated with participating in this project?

There are no foreseeable risks related to participate in this study.

What are the potential benefits of the research project?

As an appreciation of the time spent, participants who are eligible and complete the survey will receive a reimbursement, an Amazon gift card worth 10 Australian dollars. You may also request a copy of the final report by providing us your email address at the end of the survey. The email address will be stored temporarily, separated from the survey data, and deleted after sending the report.

Can I withdraw from the project?

Whilst your participation in this study is completely voluntary, you are free to withdraw any time prior to the submission of responses by closing the browser.

What will happen to my information?

We plan to store the collected data of the survey in the main researcher password protected laptop using specific identifier for each participant. After completion of the project, all data will be moved to the dedicated secure server and it will be coded, which only principle supervisor can access to them. We will use pseudonym to refer the name of participants in the reports that may be published in the future. It will mainly be published as coded data in PhD thesis, or in journal and conference papers. We will use pseudonym to refer the name of participants in the project outcomes. It is guaranteed that at all times, participants in this research will not be identified in any publication. 3 Researchers will keep data for 5 years. The acquired data will be only accessed by researchers involved in the study. Your information will only be used as described in this participant information sheet and it will only be disclosed according to the consent provided, except as required by law.

What if I have a complaint or any concerns?

The study has been approved by the Human Research Ethics Committee at the University of Adelaide (approval number H-2019-115). This research project will be conducted according to the NHMRC National Statement on Ethical Conduct in Human Research 2007 (Updated 2018). If you have questions or problems associated with the practical aspects of your participation in the project, or wish to raise a concern or complaint about the project, then you should consult the Principal Investigator. If you wish to speak with an independent person regarding concerns or a complaint, the University's policy on research involving human participants, or your rights as a participant, please contact the Human Research Ethics Committee's Secretariat on:

Phone: +61 8 8313 6028
Email: hrec@adelaide.edu.au
Post: Level 4, Rundle Mall Plaza, 50 Rundle Mall, ADELAIDE SA 5000

Any complaint or concern will be treated in confidence and fully investigated. You will be informed of the outcome.

If I want to participate, what do I do?

You only need to submit the completed response as an indication of your consent to participate.

Survey Questions

Part A: Demographic Questions

Q1. Please tell us the estimated number of mobile health apps you have developed?

☐ 0 apps ☐ 1-3 apps ☐ 4-8 apps ☐ More than 8 apps

Q2. Name one mobile health app developed and tell us about it, e.g., the purpose and how it works)?

Q3. Is the app you described above already available to download? ☐ Yes ☐ No

Q4. I work as a ☐ Full-time ☐ Part-time

Q5. Do you have any specific role? Please name it?

Q6. Please select which platform you are working on? ☐ Android. ☐ iOS. ☐ Others, please name.

Q7. How many years of experience do you have in mobile health apps development?

☐ Less than 1 year ☐ 2-4 years ☐ 5-10 years ☐ 11-15 years ☐ More than 15 years

Q8. Please tell us the approximate size of your team including yourself?

Q9. Please tell us which country you or your organisation located?

Part B: Challenges, practice, and motivations for developing secure mobile health applications

Q10. What are the challenges that you think hinder you to develop secure mobile health apps?

Q11. Please choose your level of agreement for the following challenges based on your experience in developing mobile health apps: Strongly agree, Agree, Disagree, Strongly disagree, Not sure

☐ Insufficient security knowledge (e.g., insecure coding practice, improper usage or lack of security tools, using untrusted libraries).

☐ Little or no budget for employing security.

☐ Lack of security experts involvement during the development.

☐ Poor security decisions during the development process (e.g., relying on insecure resources, developer' own assumption).

☐ The speed of delivering mobile health applications makes me leave security behind.

☐ Lack of applications security testing.

☐ Assuming that users are not that much interested in security.

☐ Assuming that security should be resolved by app testers.

Q12. What approaches you have followed/ or found useful for ensuring the security/ or resolving the security issues during the development of mobile health apps?

Q13. What motivate you to ensure you are developing secure mobile health apps?

Q14. Please choose your level of agreement for the following motivations based on your experience in developing mobile health apps: Strongly agree, Agree, Disagree, Strongly disagree, Not sure

☐ I develop secure apps because I previously experienced application failure.

☐ I develop secure apps because mobile health applications will have big impact if it is insecure.

☐ I develop secure apps to maintain the reputation of my organisation.

☐ I develop secure apps because I look for career path and promotion.

☐ I develop secure apps because I expect reward and recognition.

☐ I develop secure apps because we have security leader who influences me to develop secure apps.

Q15 (Optional). Do you have any other thoughts about the security in mobile health apps you would like to share with us?

Appendix C

Survey Instrument for End-Users' Study

Research Title: Understanding the Security Awareness of Mobile Health Applications Users: An Empirical Investigation

Ethics approval: H-2019-165

The University of Adelaide, Australia

General Information

Mobile health applications (apps) hold great promises to improve and facilitate healthcare domain. Using mobile health apps will not only improve accessing to healthcare services, but also lower its cost and increase health awareness of patients. But, security cannot be achievable solutions alone. Users' security awareness toward using mobile health apps is critical for safe and secure usage. Hence, there is a need to understand the level of security awareness of mobile health apps users' to prevent the negative impact. To assess the extent to which the users of mHealth apps are aware of the security concerns, we aim to empirically investigate and assess users' security awareness toward using mHealth apps. Our study will be conducted through a survey to allow us collect qualitative and quantitative data that can be beneficial for the research.

Who do I contact if I have questions about the project?

Any questions regarding the project and survey can be asked via:

Bakheet Aljedaani, Bakheet.aljedaani@adelaide.edu.au
Prof. Muhammad Ali Babar, ali.babr@adelaide.edu.au
Dr. Christoph Treude, Christoph.treude@adelaide.edu.au

Why am I being invited to participate?

You are being invited as you are a user for mobile health apps to participate in our study. You should be over 18 years of age and have used the mobile health apps which have been provided by the health provider. You should be able to communicate in English or Arabic to be in this study.

What am I being invited to do?

You are being invited to participate in an online survey about the app users security awareness toward using mobile health apps, and what concerns do you have when using the app. The survey contains two main sections including general questions (e.g., range of age, gender, level of education, etc.), and what security features and concerns you have been experiencing during the use of mobile health apps. The survey questions have been formulated in different forms (i.e., multiple-choice questions, Likert questions and open-ended questions) to allow you to share with us your experience toward using mHealth app. All responses will be kept anonymous.

How much time will my involvement in the project take?

Answering the survey will take approximately 10 minutes of your time. But it can take shorter or longer time.

Are there any risks associated with participating in this project?

There are no foreseeable risks related to participate in this study.

What are the potential benefits of the research project?

Participants who complete the survey with eligible responses may participate in a prize draw to win one of ten 100SR gift cards. This requires providing an email address to contact at the end of the survey. The email addresses will be securely deleted after the prize draw is held. A link for collecting email addresses will be provided at the end of the study for participants who are interested to receive the results of the survey when published. All email addresses will be stored temporarily, separate from the survey data, and securely deleted after sending our final report.

Can I withdraw from the project?

Whilst your participation in this study is completely voluntary, you are free to withdraw any time prior to the submission of responses by closing the browser.

What will happen to my information?

We plan to store the collected data of the survey in the main researcher password protected laptop as well as on the university server space using specific identifier for each participant. After completion of the project, all data will be moved to the dedicated secure server and it will be coded, which only principle supervisor can access to them. We will use pseudonym to refer the name of participants in the reports that may be published in the future. It will mainly be published as coded data in PhD thesis, or in journal and conference papers. It is guaranteed that at all times, participants in this research will not be identified in any publication. Data will be retained for a minimum of 5 years. The acquired data will be only accessed by researchers involved in the study. Your information will only be used as described in this participant information sheet and it will not be used for other studies. Your information will only be disclosed according to the consent provided, except as required by law.

Who do I contact if I have questions about the project?

Any questions regarding the project and survey can be asked via:

Bakheet Aljedaani, Bakheet.aljedaani@adelaide.edu.au
Prof. Muhammad Ali Babar, ali.babr@adelaide.edu.au
Dr. Christoph Treude, Christoph.treude@adelaide.edu.au

What if I have a complaint or any concerns?

The study has been approved by the Human Research Ethics Committee at the University of Adelaide (approval number H-2019-165). This research project will be conducted according to the NHMRC National Statement on Ethical Conduct in Human Research 2007 (Updated 2018). If you have questions or problems associated with the practical aspects of your participation in the project, or wish to raise a concern or complaint about the project, then you should consult the Principal Investigator. If you wish to speak with an independent person regarding concerns or a complaint, the University's policy on research involving human participants, or your rights as a participant, please contact the Human Research Ethics Committee's Secretariat on:

Phone: +61 8 8313 6028
Email: hrec@adelaide.edu.au
Post: Level 4, Rundle Mall Plaza, 50 Rundle Mall, ADELAIDE SA 5000

Any complaint or concern will be treated in confidence and fully investigated. You will be informed of the outcome.

If I want to participate, what do I do?

You only need to submit the completed response as an indication of your consent to participate.

Survey Questions

Part 1: Demographic questions of the participants

Q1: What is your age? ☐ 18 - 29 ☐ 30 - 49 ☐ Over 50
Q2: What is your gender? ☐ Female ☐ Male ☐ Prefer not to say
Q3: What is your level of education? ☐ High school or less ☐ Diploma ☐ Bachelor's ☐ Higher Diploma ☐ Higher education (Master's or PhD)
Q4: What is mobile OS? ☐ I use Android (e.g., Samsung) ☐ I use iOS (i.e., Apple) ☐ Others, please specify
Q5: Which apps you're using? ☐ iKFMC app ☐ HMG app
Q6: Please rate you knowledge in using information technology? ☐ Little or no knowledge at all ☐ Moderate knowledge ☐ Advanced knowledge

Part 2: Security issues of using mobile health apps

Q7: Please keep in mind that this is NOT a test. Respond to each of the following statement based on your current knowledge. Your options would be: True (T), Don't know (DK), False (F)

Major focus	Minor focus	Dimensions for measuring mHealth apps users awareness are: Knowledge (K), Attitude (A), Behaviour (B)	Given options
Privacy	Sharing health data with third parties	K: I should be informed when my health data, which have been collected by mHealth apps, are being shared with third parties.	T, DK, F
		A: I am aware that my health data, which have been collected by mHealth apps, will not be shared with third parties.	T, DK, F
		B: I get informed when my health data, which have been collected by mHealth apps, are being shared with third parties.	T, F
Access control	Accessing health data	K: I should know who access my health data and for what purpose.	T, DK, F
		A: I am aware of who access my health data and for what purpose.	T, DK, F
		B: I know who access my health data and for what purpose.	T, F
	Controlling access to health data	K: I should have control of my health data.	T, DK, F
		A: I am aware that having control of my health data is better.	T, DK, F
		B: I have control of my health data.	T, F
	Requesting access to the data of the phone.	K: I should know that some apps request access to my health data.	T, DK, F
		A: I am aware that some apps request accessing health data more than its needs.	T, DK, F
		B: I accept or deny the request based on what I think is secure.	T, F
Encryption	Encrypting health data during	K: I should know if or not my health data, which have been collected by mHealth apps, are encrypted during transmission and storing.	T, DK, F

	transmission and storing	A: I am aware that my health data, which have been collected by mHealth apps, are encrypted during transmission and storing.	T, DK, F
Authentication	Using same password for different accounts	K: I should use different passwords for different accounts and apps.	T, DK, F
		A: I am aware that using one password for different accounts and apps will make it easy for me; yet, it is insecure.	T, DK, F
		B: I use different passwords for different accounts and apps.	T, DK, F
	Using strong password	K: I should use strong password (not easy to guess) for the mHealth app.	T, DK, F
		A: I am aware that using strong password (not easy to guess) for mHealth app provides more security.	T, DK, F
		B: I use strong password (not easy to guess) for mHealth app.	T, F
	Changing the password regularly	K: I should change the password for the app regularly.	T, DK, F
		A: I am aware that changing password for the app regularly provides more security.	T, DK, F
		B: I change my password of the app regularly.	T, F

Q8: What is the importance of securing your health data within the app? Your level of agreement will be measured by the following options: Very important, Important, Neutral, Not very important, Not important at all.

Q9: Please respond to the following statements based on your experience with the mobile health application. Your level of agreement will be measured by the following options: Always, Sometimes, Rarely, Never, I don't know

#	Statement
1.	The app has very clear, readable and understandable privacy policy.
2.	The app requested my consent to share my health data.
3.	The app does not ask for more personal information than what is needed.
4.	The apps provide convenient options for authentications that support my needs.
5.	The app does not collect data without my permission.
6.	The app has very adjustable security settings and easy-to-use.
7.	The app provides a channel to contact the developer or admin to report an issue.
8.	The app has the feature of wiping all my health data if my phone is lost or stolen.

Q10: What other security features you would like to have in mHealth apps?

Q11: What are the security barriers which you have experienced while using mobile health app?

Q12: What methods have been used to make you aware of the security features of mHealth app?

Appendix D

Exit Survey for Simulation-based Attack Study

PROJECT TITLE: Understanding User's Security Behaviour towards Using Mobile Health Applications Users: An Empirical Investigation

HUMAN RESEARCH ETHICS COMMITTEE APPROVAL NUMBER: H-2021-106

Exit Survey Questions

A. ***Demographic Questions***
    1. What is your gender? Male/ Female.
    2. What is your age group? (Young adult (18 – 29)/ Adult (30- 50)/ Senior (Above 50).
    3. What is your formal education? High school or less/ Diploma/ Bachelor/ Higher education (Masters' or PhD).
    4. What is your IT knowledge level? Little or no knowledge/ Moderate/ Advanced.
    5. Which country do you currently reside in?

B. ***End-users' Security Behaviour Questions***
    6. Please tell us the reasons that make you pay attention to access permissions? If not, tell us why you don't?

Appendix E

Approved Ethics Applications

Our reference 33609
04 July 2019

THE UNIVERSITY of ADELAIDE

RESEARCH SERVICES
OFFICE OF RESEARCH ETHICS, COMPLIANCE AND INTEGRITY
THE UNIVERSITY OF ADELAIDE
LEVEL 4, RUNDLE MALL PLAZA 50
RUNDLE MALL ADELAIDE SA 5000
AUSTRALIA

TELEPHONE +61 8 8313 5137
FACSIMILE +61 8 8313 3700

Professor Ali Babar
School of Computer Science
Dear Professor Babar
ETHICS APPROVAL No: H-2019-115

PROJECT TITLE: An Empirical Study of Success and Failure Factors for Developing Secure Mobile Health Applications

The ethics application for the above project has been reviewed by the Executive, Human Research Ethics Committee and is deemed to meet the requirements of the National Statement on Ethical Conduct in Human Research 2007 (Updated 2018) involving no more than low risk for research participants.

You are authorised to commence your research on 04/07/2019

The ethics expiry date for this project is: 31/07/2022

NAMED INVESTIGATORS:

Chief Investigator:	Professor Ali Babar
Student - Postgraduate Doctorate by Research (PhD):	Mr Bakheet Hamdan M Aljedaani
Associate Investigator:	Dr Christoph Treude

CONDITIONS OF APPROVAL: Thank you for your responses to the matters raised. The revised application provided on 04/07/2019 has been approved.

Ethics approval is granted for three years and is subject to satisfactory annual reporting. The form titled Annual Report on Project Status is to be used when reporting annual progress and project completion and can be downloaded at http://www.adelaide.edu.au/research-services/oreci/human/reporting/. Prior to expiry, ethics approval may be extended for a further period.

Participants in the study are to be given a copy of the information sheet and the signed consent form to retain. It is also a condition of approval that you immediately report anything which might warrant review of ethical approval including:

- serious or unexpected adverse effects on participants, previously unforeseen events
- which might affect continued ethical acceptability of the project, proposed changes to
- the protocol or project investigators; and the project is discontinued before the expected
- date of completion.

Yours sincerely,
Professor Paul Delfabbro
Convenor
The University of Adelaide

Our reference 33899
03 September 2019

Professor Ali Babar
School of Computer Science

RESEARCH SERVICES
OFFICE OF RESEARCH ETHICS, COMPLIANCE AND INTEGRITY
THE UNIVERSITY OF ADELAIDE
LEVEL 4, RUNDLE MALL PLAZA 50
RUNDLE MALL ADELAIDE SA 5000
AUSTRALIA

TELEPHONE +61 8 8313 5137
FACSIMILE +61 8 8313 3700
EMAIL hrec@adelaide.edu.au

Dear Professor Babar

ETHICS APPROVAL No: H-2019-165

PROJECT TITLE: Understanding the security awareness of mobile health applications users: an empirical investigation

The ethics application for the above project has been reviewed by the Secretariat, Human Research Ethics Committee and is deemed to meet the requirements of the National Statement on Ethical Conduct in Human Research 2007 (Updated 2018) involving no more than low risk for research participants.

You are authorised to commence your research on: **02/09/2019**
The ethics expiry date for this project is: **30/09/2022**

NAMED INVESTIGATORS:

Chief Investigator:	Professor Ali Babar
Student – Postgraduate Doctorate by Research (PhD):	Mr Bakheet Hamdan M Aljedaani
Associate Investigator:	Dr Christoph Treude

CONDITIONS OF APPROVAL: Thank you for addressing the feedback raised. The ethics application submit on the 29th of August 2019 is approved.

Ethics approval is granted for three years and is subject to satisfactory annual reporting. The form titled Annual Report on Project Status is to be used when reporting annual progress and project completion and can be downloaded at http://www.adelaide.edu.au/research-services/oreci/human/reporting/. Prior to expiry, ethics approval may be extended for a further period.

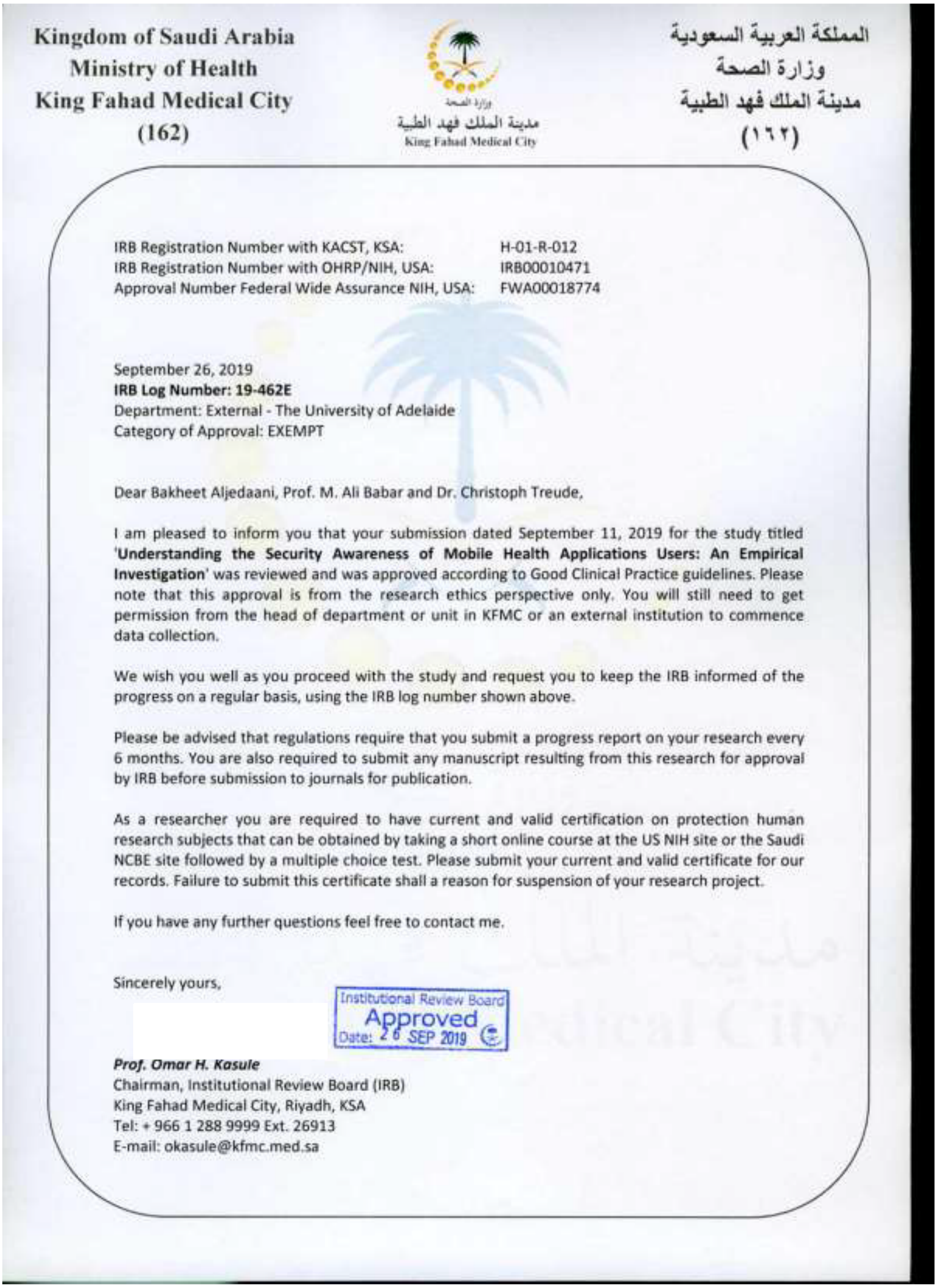
Participants in the study are to be given a copy of the information sheet and the signed consent form to retain. It is also a condition of approval that you immediately report anything which might warrant review of ethical approval including:

- serious or unexpected adverse effects on participants,
- previously unforeseen events which might affect continued ethical acceptability of
- the project, proposed changes to the protocol or project investigators; and the project
- is discontinued before the expected date of completion.

Yours sincerely,

Ms Michelle
White Secretary

The University of Adelaide



Kingdom of Saudi Arabia
Ministry of Health
King Fahad Medical City
(162)

وزارة الصحة
مدينة الملك فهد الطبية
King Fahad Medical City

المملكة العربية السعودية
وزارة الصحة
مدينة الملك فهد الطبية
(١٦٢)

IRB Registration Number with KACST, KSA:	H-01-R-012
IRB Registration Number with OHRP/NIH, USA:	IRB00010471
Approval Number Federal Wide Assurance NIH, USA:	FWA00018774

September 26, 2019
IRB Log Number: 19-462E
Department: External - The University of Adelaide
Category of Approval: EXEMPT

Dear Bakheet Aljedaani, Prof. M. Ali Babar and Dr. Christoph Treude,

I am pleased to inform you that your submission dated September 11, 2019 for the study titled '**Understanding the Security Awareness of Mobile Health Applications Users: An Empirical Investigation**' was reviewed and was approved according to Good Clinical Practice guidelines. Please note that this approval is from the research ethics perspective only. You will still need to get permission from the head of department or unit in KFMC or an external institution to commence data collection.

We wish you well as you proceed with the study and request you to keep the IRB informed of the progress on a regular basis, using the IRB log number shown above.

Please be advised that regulations require that you submit a progress report on your research every 6 months. You are also required to submit any manuscript resulting from this research for approval by IRB before submission to journals for publication.

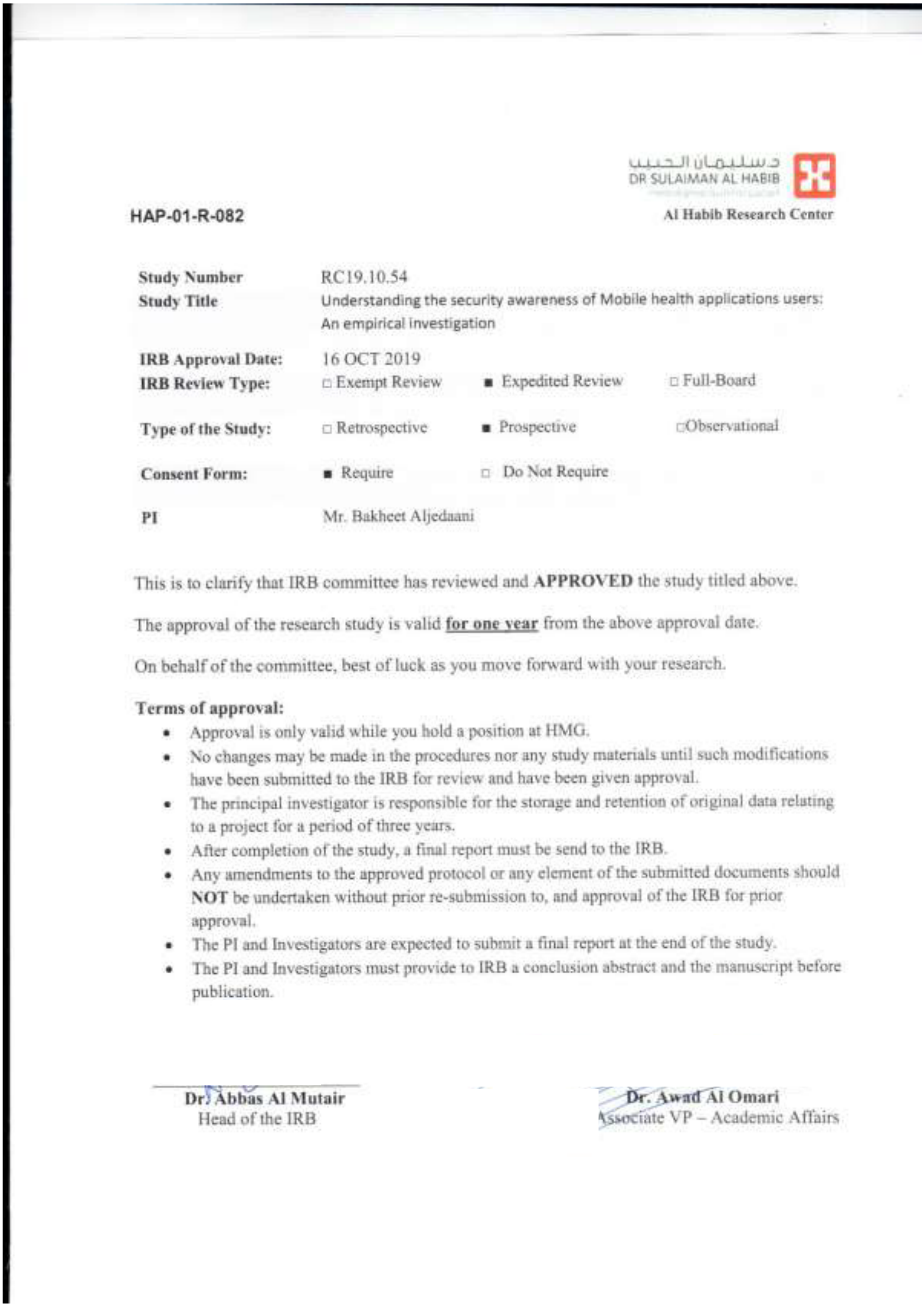
As a researcher you are required to have current and valid certification on protection human research subjects that can be obtained by taking a short online course at the US NIH site or the Saudi NCBE site followed by a multiple choice test. Please submit your current and valid certificate for our records. Failure to submit this certificate shall a reason for suspension of your research project.

If you have any further questions feel free to contact me.

Sincerely yours,

Institutional Review Board
Approved
Date: 26 SEP 2019

Prof. Omar H. Kasule
Chairman, Institutional Review Board (IRB)
King Fahad Medical City, Riyadh, KSA
Tel: + 966 1 288 9999 Ext. 26913
E-mail: okasule@kfmc.med.sa



HAP-01-R-082

د.سليمان الحبيب
DR SULAIMAN AL HABIB

Al Habib Research Center

Study Number	RC19.10.54		
Study Title	Understanding the security awareness of Mobile health applications users: An empirical investigation		
IRB Approval Date:	16 OCT 2019		
IRB Review Type:	□ Exempt Review	■ Expedited Review	□ Full-Board
Type of the Study:	□ Retrospective	■ Prospective	□Observational
Consent Form:	■ Require	□ Do Not Require	
PI	Mr. Bakheet Aljedaani		

This is to clarify that IRB committee has reviewed and **APPROVED** the study titled above.

The approval of the research study is valid **for one year** from the above approval date.

On behalf of the committee, best of luck as you move forward with your research.

Terms of approval:

- Approval is only valid while you hold a position at HMG.
- No changes may be made in the procedures nor any study materials until such modifications have been submitted to the IRB for review and have been given approval.
- The principal investigator is responsible for the storage and retention of original data relating to a project for a period of three years.
- After completion of the study, a final report must be send to the IRB.
- Any amendments to the approved protocol or any element of the submitted documents should **NOT** be undertaken without prior re-submission to, and approval of the IRB for prior approval.
- The PI and Investigators are expected to submit a final report at the end of the study.
- The PI and Investigators must provide to IRB a conclusion abstract and the manuscript before publication.

Dr. Abbas Al Mutair
Head of the IRB

Dr. Awad Al Omari
Associate VP – Academic Affairs

Our reference 35203

07 July 2021

Professor Ali Babar
School of Computer Science

THE UNIVERSITY of ADELAIDE

RESEARCH SERVICES
OFFICE OF RESEARCH ETHICS, COMPLIANCE AND INTEGRITY
THE UNIVERSITY OF ADELAIDE
LEVEL 4, RUNDLE MALL PLAZA 50
RUNDLE MALL ADELAIDE SA 5000
AUSTRALIA

TELEPHONE +61 8 8313 5137
FACSIMILE +61 8 8313 3700
EMAIL hrec@adelaide.edu.au

Dear Professor Babar

ETHICS APPROVAL No: H-2021-106

PROJECT TITLE: Understanding End-Users' Security Behaviours towards Using Mobile Health Applications: An Empirical Investigation

The ethics application for the above project has been reviewed by the Human Research Ethics Committee and is deemed to meet the requirements of the National Statement on Ethical Conduct in Human Research 2007(Updated 2018).

You are authorised to commence your research on: **07/07/2021**
The ethics expiry date for this project is: **31/07/2024**

NAMED INVESTIGATORS:

Chief Investigator: Professor Ali Babar
Student - PostgraduateDoctorate by Research (PhD): Mr Bakheet Hamdan M Aljedaani
Associate Investigator: Dr Christoph Treude

CONDITIONS OF APPROVAL:

Thank you for addressing the feedback. The revised application submitted on the 7th of July 2021 has been approved.

Ethics approval is granted for three years and is subject to satisfactory annual reporting. The form titled Annual Report on Project Status is to be used when reporting annual progress and project completion and can be downloaded at http://www.adelaide.edu.au/research-services/oreci/human/reporting/. Prior to expiry, ethics approval may be extended for a further period.

Participants in the study are to be given a copy of the information sheet and the signed consent form to retain. It is also a condition of approval that you immediately report anything which might warrant review of ethical approval including:

- serious or unexpected adverse effects on participants,
- previously unforeseen events which might affect continued ethical acceptability of the project,
- proposed changes to the protocol or project investigators; and
- the project is discontinued before the expected date of completion.

RESEARCH SERVICES

Yours sincerely,

Professor Paul Delfabbro
Convenor
The University of Adelaide

References

[1] A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, and C. Patsakis, "Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice" IEEE Access, vol. 6, pp. 9390-9403, 2018.

[2] G. Association, "The Mobile Economy available at https://www.gsma.com/mobileeconomy/" 2020, [Accessed 21-02-2022].

[3] D. Kotz, C. A. Gunter, S. Kumar, and J. P. Weiner, "Privacy and Security in Mobile Health: A Research Agenda" Computer, vol. 49, pp. 22-30, 2016.

[4] F. Zubaydi, A. Saleh, F. Aloul, and A. Sagahyroon, "Security of mobile health (mHealth) systems" in 2015 IEEE 15th International Conference on Bioinformatics and Bioengineering, BIBE 2015, 2015.

[5] K. Knorr and D. Aspinall, "Security testing for Android mHealth apps" in 2015 IEEE 8th International Conference on Software Testing, Verification and Validation Workshops, ICSTW 2015 - Proceedings, 2015.

[6] H. K. Flaten, C. St Claire, E. Schlager, C. A. Dunnick, and R. P. Dellavalle, "Growth of mobile applications in dermatology-2017 update" Dermatology online journal, vol. 24, 2018.

[7] F. Zahra, A. Hussain, and H. Mohd, "Factor Affecting Mobile Health Application for Chronic Diseases" Journal of Telecommunication, Electronic and Computer Engineering (JTEC), vol. 10, pp. 77-81, 2018.

[8] T. Mabo, B. Swar, and S. Aghili, "A vulnerability study of Mhealth chronic disease management (CDM) applications (apps) " in Advances in Intelligent Systems and Computing vol. 745, ed, 2018, pp. 587-598.

[9] L. Ramey, C. Osborne, D. Kasitinon, and S. Juengst, "Apps and Mobile Health Technology in Rehabilitation: The Good, the Bad, and the Unknown" Physical Medicine and Rehabilitation Clinics, vol. 30, pp. 485-497, 2019.

[10] Research2guide, "mHealth App Economics 2017/2018 Current Status and Future Trends in Mobile Health available at https://research2guidance.com" 2017, [Accessed 21-02-2022].

[11] O. Byambasuren, E. Beller, and P. Glasziou, "Current Knowledge and Adoption of Mobile Health Apps Among Australian General Practitioners: Survey Study" JMIR mHealth and uHealth, vol. 7, p. e13199, 2019.

[12] B. Martínez-Pérez, I. de la Torre-Díez, and M. López-Coronado, "Privacy and Security in Mobile Health Apps: A Review and Recommendations" Journal of Medical Systems, vol. 39, 2015.

[13] I. Vaghefi and B. Tulu, "The continued use of mobile health apps: insights from a longitudinal study" JMIR mHealth and uHealth, vol. 7, p. e12983, 2019.

[14] Research2guidance, "The mhealth app market will grow by 15% to reach $31 billion by 2020" 2018, [Accessed 21-02-2022].

[15] M. Hussain, A. A. Zaidan, B. B. Zidan, S. Iqbal, M. M. Ahmed, O. S. Albahri, et al., "Conceptual framework for the security of mobile health applications on Android platform" Telematics and Informatics, 2018.

[16] R. Adhikari, D. Richards, and K. Scott, "Security and privacy issues related to the use of mobile health apps" in Proceedings of the 25th Australasian Conference on Information Systems, ACIS 2014, 2014.

[17] S. Gejibo, F. Mancini, K. A. Mughal, R. A. B. Valvik, and J. Klungsøyr, "Secure data storage for mobile data collection systems" in Proceedings of the International Conference on Management of Emergent Digital EcoSystems, MEDES 2012, 2012, pp. 131-138.

[18] M. Hussain, A. A. Zaidan, B. B. Zidan, S. Iqbal, M. M. Ahmed, O. S. Albahri, et al., "Conceptual framework for the security of mobile health applications on Android platform" Telematics and Informatics, vol. 35, pp. 1335-1354, 2018.

[19] E. P. Morera, I. de la Torre Díez, B. Garcia-Zapirain, M. López-Coronado, and J. Arambarri, "Security Recommendations for mHealth Apps: Elaboration of a Developer’s Guide" Journal of Medical Systems, vol. 40, 2016.

[20] T. Anderson, "Bitglass Report available at https://globenewswire.com/news-release/2018/03/01/1402122/0/en/Bitglass-Report-Healthcare-Record-Breaches-Hit-Four-Year-Low.html," 2018.

[21] "What hackers actually do with your stolen medical records available at https://www.advisory.com/en/daily-briefing/2019/03/01/hackers" 2019, [Accessed 21-02-2022].

[22] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? Security awareness in smartphone platforms" Computers & Security, vol. 34, pp. 47-66, 2013.

[23] L. Zhou, J. Bao, V. Watzlaf, and B. Parmanto, "Barriers to and facilitators of the use of mobile health apps from a security perspective: Mixed-methods study" JMIR mHealth and uHealth, vol. 7, 2019.

[24] A. A. Atienza, C. Zarcadoolas, W. Vaughon, P. Hughes, V. Patel, W.-Y. S. Chou, et al., "Consumer attitudes and perceptions on mHealth privacy and security: findings from a mixed-methods study" Journal of health communication, vol. 20, pp. 673-679, 2015.

[25] I. Consulting, General Data Protection Regulation available at "https://gdpr-info.eu/" [Accessed 21-02-2022]

[26] J. Muchagata and A. Ferreira, "Translating GDPR into the mHealth Practice" in Proceedings - International Carnahan Conference on Security Technology, 2018.

[27] U. S. D. o. H. H. Services, "Health Information Privacy available at https://www.hhs.gov/hipaa/index.html", [Accessed 21-02-2022].

[28] D. D. Luxton, R. A. Kayl, and M. C. Mishkind, "MHealth data security: The need for HIPAA-compliant standardization" Telemedicine and e-Health, vol. 18, pp. 284-288, 2012.

[29] Y. Cifuentes, L. Beltrán, and L. Ramírez, "Analysis of Security Vulnerabilities for Mobile Health Applications" in 2015 Seventh International Conference on Mobile Computing and Networking (ICMCN 2015), 2015.

[30] L. Horn Iwaya, A. Ahmad, and M. A. Babar, "Security and Privacy for mHealth and uHealth Systems: A Systematic Mapping Study " in IEEE Access, vol. 8, pp. 150081-150112 doi: 10.1109/ACCESS.2020.3015962, 2020.

[31] L. H. Iwaya, S. Fischer-Hübner, R.-M. Åhlfeldt, and L. A. Martucci, "mhealth: A privacy threat analysis for public health surveillance systems" in 2018 IEEE 31st International Symposium on Computer-Based Medical Systems (CBMS), 2018, pp. 42-47.

[32] S. Arora, J. Yttri, and W. Nilsen, "Privacy and security in mobile health (mHealth) research" Alcohol research: current reviews, vol. 36, p. 143, 2014.

[33] S. S. Bhuyan, H. Kim, O. O. Isehunwa, N. Kumar, J. Bhatt, D. K. Wyant, et al., "Privacy and security issues in mobile health: Current research and future directions" Health Policy and Technology, vol. 6, pp. 188-191, 2017.

[34] B. Aljedaani, A. Ahmad, M. Zahedi, and M. A. Babar, "An Empirical Study on Developing Secure Mobile Health Apps: The Developers' Perspective" 27th Asia-Pacific Software Engineering Conference (APSEC), Singapore, Singapore, pp. 208-217, 2020.

[35] D. He, M. Naveed, C. A. Gunter, and K. Nahrstedt, "Security Concerns in Android mHealth Apps" AMIA ... Annual Symposium proceedings / AMIA Symposium. AMIA Symposium, vol. 2014, pp. 645-654, 2014.

[36] G. Thamilarasu and C. Lakin, "A security framework for mobile health applications" in Proceedings - 2017 5th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2017, 2017, pp. 221-226.

[37] S. M. Furnell, A. Jusoh, and D. Katsabas, "The challenges of understanding and using security: A survey of end-users" Computers & Security, vol. 25, pp. 27-35, 2006.

[38] S. Furnell, R. Esmael, W. Yang, and N. Li, "Enhancing security behaviour by supporting the user" Computers & Security, vol. 75, pp. 1-9, 2018.

[39] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The human aspects of information security questionnaire (HAIS-Q): two further validation studies" Computers & Security, vol. 66, pp. 40-51, 2017.

[40] B. Aljedaani, A. Ahmad, M. Zahedi, and M. A. Babar, "Security Awareness of End-Users of Mobile Health Applications: An Empirical Study" presented at the MobiQuitous 2020 - 17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Darmstadt, Germany, 2020.

[41] B. A. Kitchenham, T. Dyba, and M. Jorgensen, "Evidence-based software engineering" in Proceedings. 26th International Conference on Software Engineering, 2004, pp. 273-281.

[42] B. Kitchenham, R. Pretorius, D. Budgen, O. P. Brereton, M. Turner, M. Niazi, et al., "Systematic literature reviews in software engineering–a tertiary study" Information and Software Technology, vol. 52, pp. 792-805, 2010.

[43] B. Aljedaani and M. A. Babar, "Challenges With Developing Secure Mobile Health Applications: Systematic Review" JMIR Mhealth Uhealth, vol. 9, p. e15654, 2021.

[44] B. A. Kitchenham and S. L. Pfleeger, "Personal opinion surveys" in Guide to advanced empirical software engineering, ed: Springer, 2008, pp. 63-92.

[45] B. Aljedaani, "An Empirical Study on Developing Secure Mobile Health Apps: The Developers' Perspective [Supplementary Data]. [Online:] https://sites.google.com/view/mhealth-study-documents/home" 2020.

[46] L. A. Goodman, "Snowball sampling" The annals of mathematical statistics, pp. 148-170, 1961.

[47] D. S. Cruzes and T. Dyba, "Recommended steps for thematic synthesis in software engineering," in Empirical Software Engineering and Measurement (ESEM), 2011 International Symposium on, 2011, pp. 275-284.

[48] V. Braun and V. Clarke, "Using thematic analysis in psychology" Qualitative research in psychology, vol. 3, pp. 77-101, 2006.

[49] B. Aljedaani, "End-Users' Knowledge and Perception about Security of Clinical Mobile Health Apps: A Case Study with Two Saudi Arabian mHealth Providers [Supplementary Data]. [Online:] https://sites.google.com/view/end-users-study-of-mhealth-app/home" 2021.

[50] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness" Computers & security, vol. 25, pp. 289-296, 2006.

[51] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q) " Computers & security, vol. 42, pp. 165-176, 2014.

[52] B. Aljedaani, A. Ahmad, M. Zahedi, and M. A. Babar, "End-Users' Knowledge and Perception about Security of Mobile Health Apps: A Case Study with Two Saudi Arabian mHealth Providers" arXiv preprint arXiv:2101.10412, 2021.

[53] W. Peng, S. Kanthawala, S. Yuan, and S. A. Hussain, "A qualitative study of user perceptions of mobile health apps" BMC Public Health, vol. 16, p. 1158, 2016.

[54] R. Bitton, K. Boymgold, R. Puzis, and A. Shabtai, "Evaluating the Information Security Awareness of Smartphone Users" in Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 2020, pp. 1-13.

[55] S. Barth, M. D. de Jong, M. Junger, P. H. Hartel, and J. C. Roppelt, "Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources" Telematics and informatics, vol. 41, pp. 55-69, 2019.

[56] S. Egelman, M. Harbach, and E. Peer, "Behavior ever follows intention? A validation of the Security Behavior Intentions Scale (SeBIS) " in Proceedings of the 2016 CHI conference on human factors in computing systems, 2016, pp. 5257-5261.

[57] 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, 2012, pp. 1-14.

[58] E. Struse, J. Seifert, S. Üllenbeck, E. Rukzio, and C. Wolf, "PermissionWatcher: Creating User Awareness of Application Permissions in Mobile Systems" in International Joint Conference on Ambient Intelligence, 2012, pp. 65-80.

[59] P. Wijesekera, A. Baokar, A. Hosseini, S. Egelman, D. Wagner, and K. Beznosov, "Android permissions remystified: A field study on contextual integrity" in 24th {USENIX} Security Symposium ({USENIX} Security 15), 2015, pp. 499-514.

[60] B. Aljedaani, "Measuring the Security Awareness of End-Users towards Using Mobile Health Apps: An Attack Simulation Approach [Supplementary Data]. [Online:] https://sites.google.com/view/attack-simulation-approach/home" 2021.

[61] M. Tavakol and R. Dennick, "Making sense of Cronbach's alpha" International journal of medical education, vol. 2, p. 53, 2011.

[62] L. Statistics, "Chi-Square Test for Association using SPSS Statistics [online] available at https://statistics.laerd.com/spss-tutorials/chi-square-test-for-association-using-spss-statistics.php" 2018, [Accessed 21-02-2022].

[63] R. G. v. d. Berg, "SPSS Mann-Whitney Test – Simple Example available at https://www.spss-tutorials.com/spss-mann-whitney-test-simple-example/" 2020, [Accessed 21-02-2022].

[64] S. Glen, "Kruskal Wallis H Test: Definition, Examples & Assumptions available at https://www.statisticshowto.com/kruskal-wallis/" 2021, [Accessed 21-02-2022].

[65] L. Statistics, "Kruskal-Wallis H Test using SPSS Statistics [online] available at https://statistics.laerd.com/spss-tutorials/kruskal-wallis-h-test-using-spss-statistics.php" 2018, [Accessed 21-02-2022].

[66] J. Müthing, T. Jäschke, and C. M. Friedrich, "Client-Focused Security Assessment of mHealth Apps and Recommended Practices to Prevent or Mitigate Transport Security Issues" JMIR mHealth and uHealth, vol. 5, 2017.

[67] U. Varshney, "Mobile health: Four emerging themes of research," Decision Support Systems, vol. 66, pp. 20-35, 2014.

[68] E. M. Chin, "Helping developers construct secure mobile applications," UC Berkeley, 2013.

[69] Research2guidance, "2017. mHealth app Economics: Current Status and Future Trends in Mobile Health available at https://research2guidance.com/product/mhealth-economics-2017-current-status-and-future-trends-in-mobile-health/" [Accessed 21-02-2022].

[70] C. Weir, B. Hermann, and S. Fahl, "From Needs to Actions to Secure Apps? The Effect of Requirements and Developer Practices on App Security" in 29th {USENIX} Security Symposium ({USENIX} Security 20), 2020.

[71] T. L. Lewis and J. C. Wyatt, "mHealth and mobile medical apps: a framework to assess risk and promote safer use" Journal of medical Internet research, vol. 16, 2014.

[72] T. Dehling, F. Gao, S. Schneider, and A. Sunyaev, "Exploring the far side of mobile health: information security and privacy of mobile health apps on iOS and Android" JMIR mHealth and uHealth, vol. 3, 2015.

[73] S. L. Kanniah and M. N. r. Mahrin, "A Review on Factors Influencing Implementation of Secure Software Development Practices" World Academy of Science, Engineering and Technology, International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering, vol. 10, pp. 3022-3029, 2016.

[74] T. W. Thomas, M. Tabassum, B. Chu, and H. Lipford, "Security During Application Development: an Application Security Expert Perspective" in Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 2018, p. 262.

[75] V. Raghavan and X. Zhang, "Building security in during information systems development" AMCIS 2009 Proceedings, p. 687, 2009.

[76] C. Weir, A. Rashid, and J. Noble, "Developer Essentials: Top Five Interventions to Support Secure Software Development" 2017.

[77] Y. Acar, C. Stransky, D. Wermke, C. Weir, M. L. Mazurek, and S. Fahl, "Developers Need Support, Too: A Survey of Security Advice for Software Developers" in Cybersecurity Development (SecDev), 2017 IEEE, 2017, pp. 22-26.

[78] I. A. Chatzipavlou, S. A. Christoforidou, and M. Vlachopoulou, "A recommended guideline for the development of mHealth Apps" Mhealth, vol. 2, 2016.

[79] J. Katusiime and N. Pinkwart, "A review of privacy and usability issues in mobile health systems: Role of external factors" Health Informatics Journal, vol. 25, pp. 935-950, 2019.

[80] G. Marquez, H. Astudillo, and C. Taramasco, "Security in Telehealth Systems from a Software Engineering Viewpoint: A Systematic Mapping Study" IEEE Access, vol. 8, pp. 10933-10950, 2020.

[81] P. A. Regoniel, "Conceptual framework: A step by step guide on how to make one" SimplyEducate. Me, 2015.

[82] S. Barnum and G. McGraw, "Knowledge for software security" IEEE Security & Privacy, vol. 3, pp. 74-78, 2005.

[83] L. Nurgalieva, D. O'Callaghan, and G. Doherty, "Security and Privacy of mHealth Applications: A Scoping Review" IEEE Access, vol. 8, pp. 104247-104268, 2020.

[84] H. Assal and S. Chiasson, "'Think secure from the beginning' A Survey with Software Developers" in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 2019, pp. 1-13.

[85] C. Weir, A. Rashid, and J. Noble, "How to Improve the Security Skills of Mobile App Developers: Comparing and Contrasting Expert Views" 2016.

[86] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications" arXiv preprint arXiv:1802.02041, 2018.

[87] S. Faily, "Engaging Stakeholders in Security Design: An Assumption-Driven Approach" 2014.

[88] G. Wurster and P. C. van Oorschot, "The developer is the enemy" in Proceedings of the 2008 New Security Paradigms Workshop, 2009, pp. 89-97.

[89] D. C. Nguyen, D. Wermke, Y. Acar, M. Backes, C. Weir, and S. Fahl, "A Stitch in Time: Supporting Android Developers in Writing Secure Code" 2017.

[90] R. Balebako, A. Marsh, J. Lin, J. I. Hong, and L. F. Cranor, "The privacy and security behaviors of smartphone app developers" 2014.

[91] G. McGraw, "Software security: building security in" vol. 1: Addison-Wesley Professional, 2006.

[92] M. Howard and S. Lipner, "The security development lifecycle" vol. 8: Microsoft Press Redmond, 2006.

[93] I. M. Woon and A. Kankanhalli, "Investigation of IS professionals' intention to practise secure development of applications" International Journal of Human-Computer Studies, vol. 65, pp. 29-41, 2007.

[94] "Ponemon Institute LLC. 2015. The State of Mobile Application Insecurity available at "https://www.workplaceprivacyreport.com/wp-content/uploads/sites/162/2015/03/WGL03074USEN.pdf" , [Accessed 21-02-2022].

[95] "National cyber security centre. 2017. Secure development is everyone's concern available at "https://www.ncsc.gov.uk/guidance/secure-development-everyones-concern", [Accessed 21-02-2022].

[96] V. N. Inukollu, D. D. Keshamoni, T. Kang, and M. Inukollu, "Factors influencing quality of mobile apps: Role of mobile app development life cycle," arXiv preprint arXiv:1410.4537, 2014.

[97] H. Sharp, N. Baddoo, S. Beecham, T. Hall, and H. Robinson, "Models of motivation in software engineering" Information and software technology, vol. 51, pp. 219-233, 2009.

[98] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: managing security behaviour in organisations" in Proceedings of the 2008 New Security Paradigms Workshop, 2009, pp. 47-58.

[99] J. M. Verner, M. A. Babar, N. Cerpa, T. Hall, and S. Beecham, "Factors that motivate software engineering teams: A four country empirical study" Journal of Systems and Software, vol. 92, pp. 115-127, 2014.

[100] J. Xie, H. R. Lipford, and B. Chu, "Why do programmers make security errors? " in Visual Languages and Human-Centric Computing (VL/HCC), 2011 IEEE Symposium on, 2011, pp. 161-164.

[101] Y. Jabareen, "Building a conceptual framework: philosophy, definitions, and procedure" International journal of qualitative methods, vol. 8, pp. 49-62, 2009.

[102] A. A. Khan, J. Keung, S. Hussain, M. Niazi, and M. M. I. Tamimy, "Understanding software process improvement in global software development: a theoretical framework of human factors" ACM SIGAPP Applied Computing Review, vol. 17, pp. 5-15, 2017.

[103] M. Niazi, D. Wilson, and D. Zowghi, "Critical success factors for software process improvement implementation: an empirical study" Software Process: Improvement and Practice, vol. 11, pp. 193-211, 2006.

[104] N. Baddoo, "Motivators and de-motivators in software process improvement: an empirical study" 2001.

[105] N. c. s. centre, "Secure development is everyone's concern available at https://www.ncsc.gov.uk/guidance/secure-development-everyones-concern" 2017, [Accessed 21-02-2022].

[106] M. Shahin, M. A. Babar, and L. Zhu, "Continuous integration, delivery and deployment: a systematic review on approaches, tools, challenges and practices" IEEE Access, vol. 5, pp. 3909-3943, 2017.

[107] S. Marsh, Y. Wang, S. Noel, L. Robart, and J. Stewart, "Device Comfort for mobile health information accessibility" in 2013 11th Annual Conference on Privacy, Security and Trust, PST 2013, 2013, pp. 377-380.

[108] L. State, "The rise of mHealth apps: A market snapshot available at https://liquid-state.com/mhealth-apps-market-snapshot/" 2018, [Accessed 21-02-2022].

[109] Z. m. research, "Global mHealth apps market available at "https://www.globenewswire.com/news-release/2019/01/24/1704860/0/en/Global-mHealth-Apps-Market-Will-Reach-USD-111-1-Billion-By-2025-Zion-Market-Research.html" 2019, [Accessed 21-02-2022].

[110] S. R. Ugalmugale. S, "mHealth Market Growth Statistics 2019-2025 available at https://www.gminsights.com/industry-analysis/mhealth-market" 2019, [Accessed 21-02-2022].

[111] T. t. c. o. death, "Top 10 causes of death worldwide available at www.who.int/mediacentre/factsheets/fs310/en/" 2017.

[112] Verizon, "Verizon Data Breach Investigation Report available at https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf" 2018, [Accessed 21-02-2022].

[113] M. Plachkinova, S. Andres, and S. Chatterjee, "A Taxonomy of mHealth apps - Security and privacy concerns," in Proceedings of the Annual Hawaii International Conference on System Sciences, 2015, pp. 3187-3196.

[114] L. Parker, V. Halter, T. Karliychuk, and Q. Grundy, "How private is your mental health app data? An empirical study of mental health app privacy policies and practices" International Journal of Law and Psychiatry, vol. 64, pp. 198-204, 2019.

[115] L. Zhou, B. Parmanto, Z. Alfikri, and J. Bao, "A Mobile App for Assisting Users to Make Informed Selections in Security Settings for Protecting Personal Health Data: Development and Feasibility Study" JMIR Mhealth Uhealth, vol. 6, p. e11210, 2018.

[116] T. A. Wani, A. Mendoza, and K. Gray, "BYOD in Hospitals-Security Issues and Mitigation Strategies" in ACM International Conference Proceeding Series, 2019.

[117] "Sample Privacy Policy Template available at "https://www.termsfeed.com/blog/sample-privacy-policy-template/" June 2020, [Accessed 21-02-2022].

[118] J. Nicholas, A. S. Fogarty, K. Boydell, and H. Christensen, "The reviews are in: A qualitative content analysis of consumer perspectives on apps for bipolar disorder," Journal of Medical Internet Research, vol. 19, 2017.

[119] A. M. Bauer, M. Iles-Shih, R. H. Ghomi, T. Rue, T. Grover, N. Kincler, et al., "Acceptability of mHealth augmentation of Collaborative Care: A mixed methods pilot study" General Hospital Psychiatry, vol. 51, pp. 22-29, 2018.

[120] A. Turner, "How Many People Have Smartphones In The World? available at https://www.bankmycell.com/blog/how-many-phones-are-in-the-world" 2021, [Accessed 21-02-2022].

[121] H. Molyneaux, E. Stobert, I. Kondratova, and M. Gaudet, "Security Matters… Until Something Else Matters More: Security Notifications on Different Form Factors" in International Conference on Human-Computer Interaction, 2020, pp. 189-205.

[122] R. Wash, E. Rader, and C. Fennell, "Can people self-report security accurately? Agreement between self-report and behavioral measures" in Proceedings of the 2017 CHI conference on human factors in computing systems, 2017, pp. 2228-2232.

[123] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, "A survey of cyber-security awareness in Saudi Arabia" in 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 2016, pp. 154-158.

[124] M. Zeybek, E. N. Yılmaz, and İ. A. Doğru, "A Study on Security Awareness in Mobile Devices" in 2019 1st International Informatics and Software Engineering Conference (UBMYK), 2019, pp. 1-6.

[125] B. Watson and J. Zheng, "On the user awareness of mobile security recommendations" in Proceedings of the SouthEast Conference, 2017, pp. 120-127.

[126] V. Gkioulos, G. Wangen, S. K. Katsikas, G. Kavallieratos, and P. Kotzanikolaou, "Security awareness of the digital natives" Information, vol. 8, p. 42, 2017.

[127] S. Chen, T. Su, L. Fan, G. Meng, M. Xue, Y. Liu, et al., "Are mobile banking apps secure? what can be improved?" in Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, 2018, pp. 797-802.

[128] M. Aliasgari, M. Black, and N. Yadav, "Security vulnerabilities in mobile health applications" in 2018 IEEE Conference on Application, Information and Network Security, AINS 2018, 2019, pp. 21-26.

[129] L. H. Iwaya, A. Ahmad, and M. Ali Babar, "Security and Privacy for mHealth and uHealth Systems: A Systematic Mapping Study" IEEE Access, vol. 8, pp. 150081-150112, 2020.

[130] E. S. Landman A, Carlile N, Rosenthal DI, Semakov S, Pallin DJ, Poon EG, "A Mobile App for Securely Capturing and Transferring Clinical Images to the Electronic Health Record: Description and Preliminary Usability Study available at "http://mhealth.jmir.org/2015/1/e1/" 2015.

[131] S. Becker, T. Miron-Shatz, N. Schumacher, J. Krocza, C. Diamantidis, and U.-V. Albrecht, "mHealth 2.0: experiences, possibilities, and perspectives" JMIR mHealth and uHealth, vol. 2, p. e24, 2014.

[132] F. Fischer, K. Böttinger, H. Xiao, C. Stransky, Y. Acar, M. Backes, et al., "Stack overflow considered harmful? the impact of copy&paste on android application security" in 2017 IEEE Symposium on Security and Privacy (SP), 2017, pp. 121-136.

[133] A. Saini, "How much do bugs cost to fix during each phase of the SDLC? available at https://www.synopsys.com/blogs/software-security/cost-to-fix-bugs-during-each-sdlc-phase/" 2017, [Accessed 21-02-2022].

[134] M. H. Van Velthoven, J. Smith, G. Wells, and D. Brindley, "Digital health app development standards: a systematic review protocol" BMJ open, vol. 8, p. e022969, 2018.

[135] Research2guidance, "mHealth app Economics: Current Status and Future Trends in Mobile Health retrieved from https://research2guidance.com/product/mhealth-economics-2017-current-status-and-future-trends-in-mobile-health/" 2017/2018, [Accessed 21-02-2022].

[136] R. Bitton, A. Finkelshtein, L. Sidi, R. Puzis, L. Rokach, and A. Shabtai, "Taxonomy of mobile users' security awareness" Computers & Security, vol. 73, pp. 266-293, 2018.

[137] H. Vakhnenko, "Mobile Healthcare App Development - Future of Healthcare [Online:] https://agilie.com/en/blog/mobile-healthcare-app-development-future-of-healthcare" 2019, [Accessed 21-02-2022].

[138] M. Sajjad, A. A. Abbasi, A. Malik, A. B. Altamimi, and I. M. Alseadoon, "Classification and mapping of adaptive security for mobile computing" IEEE Transactions on Emerging Topics in Computing, 2018.

[139] M. Koyuncu and T. Pusatli, "Security Awareness Level of Smartphone Users: An Exploratory Case Study" Mobile Information Systems, vol. 2019, 2019.

[140] P. K. Sari, "Measuring Information Security Awareness of Indonesian Smartphone Users," Telkomnika, vol. 12, 2014.

[141] D. Price, "Are Frequent Password Changes Actually Good for Your Security? available at https://www.makeuseof.com/tag/frequent-password-changes/", 2018 [Accessed 21-02-2022].

[142] SANS, "Time for Password Expiration to Die available at https://www.sans.org/security-awareness-training/blog/time-password-expiration-die" 2019, [Accessed 21-02-2022].

[143] SPECOPS, "NIST Password Standards available at https://specopssoft.com/blog/nist-password-standards/" 2020, [Accessed 21-02-2022].

[144] B. Aljedaani, "An Empirical Study on End-Users' Security Perspective Towards Using Mobile Health Apps [Supplementary Data]. [Online:] https://sites.google.com/view/end-users-views-of-mhealth-app/home" 2020.

[145] "Pearson's Product-Moment Correlation using SPSS Statistics available at https://statistics.laerd.com/spss-tutorials/pearsons-product-moment-correlation-using-spss-statistics.php" 2018, [Accessed 21-02-2022].

[146] K. Knorr and D. Aspinall, "Security testing for Android mHealth apps" in 2015 IEEE Eighth International Conference on Software Testing, Verification and Validation Workshops (ICSTW), 2015, pp. 1-8.

[147] I. C. S. Institute, "Usable Security and Privacy available at https://www.icsi.berkeley.edu/icsi/groups/privacy", [Accessed 21-02-2022]

[148] Microsoft, "Authentication flows available at https://docs.microsoft.com/en-us/azure/active-directory/develop/msal-authentication-flows" 2020, [Accessed 21-02-2022].

[149] M. Plachkinova, S. Andrés, and S. Chatterjee, "A Taxonomy of mHealth Apps--Security and Privacy Concerns" in System Sciences (HICSS), 2015 48th Hawaii International Conference on, 2015, pp. 3187-3196.

[150] A. M. Research, "Digital Health Market available at https://www.alliedmarketresearch.com/digital-health-market-A10934" 2021, [Accessed 21-02-2022].

[151] I. Technologies, "Hackers increasingly exploit human factor avaliable at https://www.ipctech.com/hackers-increasingly-exploit-human-factor/" 2021.

[152] UCLA, "What does Cronbach's alpha mean? available at "https://stats.idre.ucla.edu/spss/faq/what-does-cronbachs-alpha-mean/" 2021, [Accessed 21-02-2022].

[153] K. S. Taber, "The use of Cronbach's alpha when developing and reporting research instruments in science education" Research in science education, vol. 48, pp. 1273-1296, 2018.

[154] T. L. Team, "Mobile App Privacy Policy Template available at "https://termly.io/resources/templates/app-privacy-policy/#what-is-an-app-privacy-policy" 2017, [Accessed 21-02-2022].

[155] Y. Bertrand, K. Boudaoud, and M. Riveill, "What do you think about your company's leaks? A survey on end-users perception towards data leakage mechanisms" Frontiers in big Data, vol. 3, p. 38, 2020.

[156] B. Hainzinger, "How to avoid mobile phone apps from leaking your personal data available at https://appdevelopermagazine.com/how-to-avoid-mobile-phone-apps-from-leaking-your-personal-data/" 2020, [Accessed 21-02-2022].

[157] T. Germain, "How to Protect Yourself From Camera and Microphone Hacking available at https://www.consumerreports.org/privacy/how-to-protect-yourself-from-camera-and-microphone-hacking-a1010757171/" 2019, [Accessed 21-02-2022].

[158] A. Razaghpanah, R. Nithyanand, N. Vallina-Rodriguez, S. Sundaresan, M. Allman, C. Kreibich, et al., "Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem" in The 25th Annual Network and Distributed System Security Symposium (NDSS 2018), 2018.

[159] F. Mobile, "App Permissions – The Good, The Bad, and Why You Need to Pay Attention available at "https://www.finjanmobile.com/app-permissions-the-good-the-bad-and-why-you-need-to-pay-attention/" 2017, [Accessed 21-02-2022].

[160] N. Steinfeld, "“I agree to the terms and conditions”:(How) do users read privacy policies online? An eye-tracking experiment" Computers in human behavior, vol. 55, pp. 992-1000, 2016.

[161] A. P. Felt, S. Egelman, M. Finifter, D. Akhawe, and D. A. Wagner, "How to Ask for Permission" HotSec, vol. 12, pp. 7-7, 2012.