Assessing User Concerns and Preferences in the Evolution of Mobile Health Applications in Saudi Arabia

Aziz Alshehri *, Jebreel Omar Alamari, and Khalid Ali Almarhabi

Computers Department, College of Engineering and Computing, Umm Al-Qura University, Al Qunfudhah, Saudi Arabia
Email: aaashehri@uqu.edu.sa (A.A.); joammarey@uqu.edu.sa (J.O.A.); Kamarhabi@uqu.edu.sa (K.A.A.)
*Corresponding author

***Abstract*—In Saudi Arabia's rapidly growing mobile health (mHealth) sector, understanding user preferences, privacy concerns, and engagement is vital for creating user-friendly health technologies. This study explores user attitudes toward mobile health applications by addressing three key questions: What are users' main privacy concerns? How do demographics affect preferences and usage? What security and access methods do users prefer? The study involved three phases: designing a detailed survey, gathering responses from 357 users across Saudi Arabia, and analyzing the data using statistical tools. The survey covered demographics, privacy concerns, app permissions, preferred access methods, and data security. Results showed that privacy is a top priority, with most users hesitant to share sensitive health data with third parties. Users preferred sharing basic demographic information over sensitive data, such as location. Strong security measures like multi-factor authentication and data encryption were widely favored. Demographic factors, especially age and education, influenced these preferences, while gender had little impact. The study emphasizes the need for secure, transparent, and user-centered mHealth app designs. It provides valuable insights for developers and policymakers to build trust and enhance user experience in Saudi Arabia's mHealth landscape.**

***Keywords*—mobile health apps, user perceptions, privacy, security, Saudi Arabia, data encryption, multi-factor authentication, health technology**

I. Introduction

The Kingdom of Saudi Arabia pays great attention to prevention, health and physical care, and considers that attention to human health is a fundamental and a key matter for its societal renaissance. The Kingdom began to provide social services that rely mainly on fitness monitoring and smart healthcare by the mobile computing to provide many context-aware [1].

During the Corona (COVID-19) pandemic, residents in the Kingdom of Saudi Arabia found great support from the state in adopting the use of mobile phone applications on a daily basis in performing their daily work, the most important of which are smart health applications. These applications received great attention, and became the primary concern of the individual, which made every entity in the health sector concerned with launching one or more applications to care for the individual's health condition.

Some previous studies have documented that due to the increase in population around the world, which has reached 7.8 billion so far in 2023, mobile phone devices have become an integral part of an individual's life and help him monitor his health condition and manage his healthy day, as the number of subscribers to mobile phone services has reached 8.8 million subscribers. Since mobile devices are the closest to use in all countries of the Kingdom, they have been used to provide more comprehensive and context-sensitive services by unifying wireless networks that transmit device data, installed software (for processing contextual data), and finally built-in sensors (for sensing context). Hence, the use of mobile computing increased, and this concept began to spread, and many challenges arose around it.

Mobile computing has revolutionized the healthcare sector and has become the basis of all mobile health applications (mHealth applications) delivered to end users in smart healthcare initiatives [2, 3]. The goal of these applications is to provide health care services in a digital, effective, and cost-effective way by creating a line of communication between individuals and the health care industry using communication technologies in mobile phones [4]. With the increasing number of users of mHealth technologies, the market size in 2022 reached $200 billion, with an expected growth of $1069.13 billion by 2032. Based on these forecasts, the compound annual growth rate is likely to increase by 18.30% from 2023 to 2032 [5–7].

The World Health Organization (WHO) has defined mobile health applications (mHealth) as a medical and public health practice that uses mobile phones and wireless devices [8]. The service of these applications is represented by voice and short messaging services and health applications that manage the requirements for

Manuscript received November 6, 2024; revised December 12, 2024; accepted December 26, 2024; published April 16, 2025.

providing health care services. These applications are used to provide claims and advice regarding health conditions to their users, facilitate the collection and exchange of health data, and provide health care to the application user [9].

The security of vital health data that is sent and stored on these applications is one of the most important challenges facing sustainability in the use of these applications. [1, 10–14]. The risk of these applications being exposed to hackers and cyber-attacks increases, which exposes important health data such as: patient's personal data, diagnosis of his disease, results, and clinical reports to theft as a result of their high value on the black market [15]. Healthcare data is being sold on the black market for up to $250 per record according to a 2019 Trustwave Global Security report [16] and for up to $1000 per record according to Experian [17]. As awareness about privacy and security increased in the Kingdom, its trends and desire to increase efficiency and privacy increased.

Referring to the National Committee for Vital and Health Statistics' statement on the differences between privacy, security and confidentiality, we find that an individual's privacy means his right to control the writing, erasing, use, showing and hiding of his health data. While confidentiality is described as ensuring that the other party maintains the privacy of the first party's data and ensures that it is not used illegally. As for security, it includes the physical, administrative, or technological tools and safeguards that are used to protect health data [18].

Therefore, the approach that the Kingdom wants to adopt regarding the security and privacy of mHealth applications depends on building a secure and private application from the perspective of developers and the perspective of end users, in terms of security-aware of development and security-aware usability by the user. Some end users of the app may be fooled in many cases due to difficulty in understanding the security features and this gives a great opportunity for hackers to mislead users through app permissions to reveal confidential data which makes their data easy and accessible to hackers.

Because of that, developers rely on the Secure Software Development Life Cycle (SDLC) practice to design mHealth applications by implementing data encryption methods, implementing security requirements, and addressing security vulnerabilities [19]. Developers are also working on studying secure mobile maps and address records from mHealth applications to understand and measure the security awareness of end users by measuring the rate of exposure to security attacks relative to login areas according to geographic maps [20].

This study focused on exploring several key aspects of user interaction with healthcare apps. The primary research questions guiding this investigation were:

- RQ-1: What are the privacy preferences and awareness among users regarding healthcare apps? This question aims to delve into the general attitudes and concerns users have about data privacy in the context of healthcare app usage.
- RQ-2: How do demographic factors influence user comfort levels with app permissions in healthcare applications? This inquiry seeks to understand how different demographic characteristics, such as age, gender, education, and occupation, affect users' comfort and trust in granting various permissions to healthcare apps.
- RQ-3: What preferences do users have regarding access methods and data security in healthcare apps? This question focuses on identifying user preferences for accessing healthcare apps, like using passwords or biometrics, and their concerns about data security and encryption.

A three-phase methodology was employed in this study, which was based on the responses of a sample of 357 users of healthcare applications in the Kingdom of Saudi Arabia. The study aims to provide insights into the basic privacy preferences of users, how demographic factors influence these preferences and comfort levels, and the impact of access methods and data security concerns on user engagement with healthcare apps.

The remainder of this paper is structured as follows: Section II reviews related literature on mHealth applications, focusing on global adoption, privacy concerns, and user engagement. Section III outlines the research methodology, including survey design, data collection, and analysis procedures. Section IV presents the results of the data analysis. Section V provides a discussion of the key findings. Section VI concludes the paper and offers suggestions for future work.

II. Literature Review

A. Global Adoption of mHealth Applications

Several studies have explored the widespread adoption of mHealth applications across different regions. For example, Stephani *et al*. [21] conducted a global analysis highlighting the increased use of mHealth apps in chronic disease management, particularly in low- and middle-income countries where healthcare access is limited. Similarly, Kumar and Smith [22] emphasized the role of mHealth apps in supporting remote patient monitoring during the COVID-19 pandemic.

Privacy and security remain critical concerns in mHealth app deployment. Research by Lee and Park [23] investigated data breaches in major health apps, identifying common vulnerabilities in data transmission protocols. In another study, Johnson *et al*. [24] evaluated the effectiveness of end-to-end encryption in protecting sensitive health data, concluding that robust encryption standards are necessary but often inconsistently implemented.

User engagement is pivotal to the success of mHealth applications. Lopez and Torres [25] found that multilingual support in mHealth apps improved accessibility and user experience in diverse populations.

Emerging technologies have further advanced mHealth applications. Artificial Intelligence (AI) and machine learning have enabled predictive analytics in health monitoring, as discussed by Chen *et al*. [26]. Blockchain

technology, explored by Patel *et al*. [27], has also gained attention for enhancing data integrity and fostering decentralized health record management.

B. Security Awareness and Challenges

Several prior studies have examined end-users' security awareness and its associated challenges. Papageorgiou *et al*. [1] conducted a comprehensive analysis of the privacy and security aspects of popular free mobile health applications. Their study involved both dynamic and static analyses, complemented by ad hoc functionality testing of individual apps. The findings revealed that most applications analyzed failed to comply with legal data protection principles, restrictions, and directives, thereby exposing millions of users to potential data breaches. Additionally, previous research [3, 11, 21, 22] emphasized users' limited knowledge about essential security and privacy features in healthcare applications. This lack of awareness can hinder informed decision-making during the registration process, potentially discouraging users from using apps that do not adhere to established privacy and security standards.

C. Privacy Concerns Across Demographics

Plachkinova *et al*. [28] proposed a comprehensive taxonomy for classifying mHealth apps based on their privacy and security characteristics, which helps identify app vulnerabilities and assess compliance with best practices. In a related study, Parker *et al*. [29] conducted an empirical investigation into mental health apps, uncovering inconsistencies between app privacy policies and their actual data handling behaviors, raising serious concerns about user data protection in practice.

Schroeder *et al*. [30] conducted a study aimed at understanding and analyzing privacy concerns among adults using mobile applications, including mHealth and smart speaker apps. The study involved 20 participants aged 45 to 70 years over a six-month period. Researchers evaluated how participants' data privacy concerns influenced their acceptance of these technologies and their future behavior regarding continued usage. The findings indicated that older adults were initially highly concerned about data privacy risks. However, these concerns gradually diminished with prolonged app usage.

Zhou *et al*. [31] explored users' preferred privacy protection methods in mHealth applications, the reasons behind these preferences, and concerns about less favored methods. The study involved 40 participants selected according to IRB-approved criteria. Participants were presented with five privacy protection strategies through a questionnaire and chose their preferred methods based on personal reasoning. The results showed that users had significant privacy concerns about healthcare applications. However, these concerns could be alleviated by implementing customizable privacy protection modules within multi-purpose applications. Customization could be performed either through a web portal or within the application itself, ensuring stronger privacy safeguards.

Dang *et al*. [32] examined privacy concerns, intentions to disclose health information in mHealth apps, and the role of social support. A questionnaire was administered to 253 randomly selected participants. Results revealed that users displayed heightened sensitivity toward disclosing health information, with greater privacy concerns reducing their willingness to share such data. The study highlighted that individual characteristics, especially the types of social support, significantly influenced privacy concerns. Informational support was found to reduce the negative impact of perceived sensitivity of health information on privacy concerns, thereby encouraging users to disclose information. Conversely, emotional support did not demonstrate a direct moderating effect on the relationship between privacy concerns and disclosure intentions. The authors concluded that social support plays a crucial role in alleviating privacy concerns and mitigating their negative effects on users' willingness to share health information

D. Unified Security Mechanisms

Several studies [33–40] have explored users' security and privacy concerns related to health applications. Their findings emphasize the critical need for a unified mechanism to classify mobile health applications based on security and privacy standards. Such a framework could boost user confidence and alleviate concerns about data protection.

An analysis of these studies reveals that users across all age groups experience significant fears about sharing personal and health-related data through smart health applications. In some cases, these concerns prompt users to avoid such apps altogether, opting instead for direct interactions with hospitals and healthcare providers. Several studies have suggested that educating users about the security and privacy features of health applications, including potential risks and benefits, can mitigate these concerns. Additionally, many studies recommend implementing customizable privacy protection modules, accessible through either web portals or the applications themselves, as an effective way to strengthen data security.

Raising users' awareness and understanding of privacy and security policies has also been identified as a key factor in preventing data theft. Informed users are better equipped to accept or reject specific privacy agreements, thereby reducing potential vulnerabilities. Some studies even propose storing patient data in state-managed central repositories to ensure compliance with stringent security and privacy regulations, minimizing the risk of data breaches.

Given these findings, our research aims to investigate privacy preferences and concerns among healthcare system users in the Kingdom of Saudi Arabia (KSA). We seek to compare these insights with prior international studies, design a smart health system tailored to local preferences, and assess its impact on users' trust and willingness to adopt the system.

To our knowledge, previous research has primarily focused on users' desires and concerns outside the KSA. Considering the unique cultural, environmental, and

lifestyle differences among countries, understanding the specific preferences and concerns of healthcare application users in the KSA remains an unexplored area. This study addresses that gap by focusing on the context-specific needs of healthcare system users in the Kingdom.

III. Methodology

Embarking on a journey to unravel the user perceptions towards mobile health apps in Saudi Arabia, our research sails through three pivotal phases, each meticulously designed to guide us towards insightful discoveries. The beacon that lights our way consists of three Research Questions (RQs), aiming to uncover the depth and breadth of privacy preferences and concerns among users of the nation's healthcare system.

- RQ1: What are the primary privacy preferences and concerns among users?
- RQ2: How demographic factors influence user engagement and preferences in health apps?
- RQ3: What preferences do users have regarding access methods and data security in health apps?

Surveys stand as a bridge between user experiences and research findings, offering a pathway for user perceptions to illuminate our research. Through this methodology, we seek not merely to observe but to understand, to peer into the experiences, desires, and apprehensions of users, ensuring that the technology developed is not just innovative but resonates deeply with the needs and expectations of its users.

The research methodology was implemented in three distinct stages: (1) Survey design and development, (2) Data collection and participant recruitment, and (3) Data analysis and interpretation, culminating in the extraction of key findings. The research methodology is illustrated in Fig. 1, which outlines the three main phases of the study.

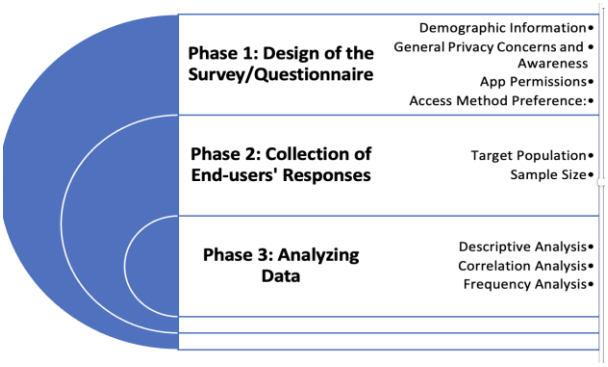

Fig. 1. Research methodology phases.

A. Phase 1: Design of the Survey/Questionnaire

The initial phase of the research methodology cantered on developing a survey instrument strategically aligned with the core objectives outlined in the research questions. Informed by a comprehensive literature review, the survey questions were specifically designed to resonate with existing research and facilitate data extraction relevant to the study. To enable nuanced analysis and targeted responses to each research question, the questionnaire was segmented into distinct thematic categories.

1) Demographic information subsection

Encompassing aspects like Gender, Age, Level of Education, and Job, we sought to understand the basic profile of our respondents, which can later be used to explore correlations or patterns in the responses.

2) General privacy concerns and awareness

Questions related to concerns about sharing healthcare records and privacy when using healthcare apps (e.g., "How concerned are you to share your healthcare records with a third party? For ads?", "Your concern when share data with health app") were included to gauge general attitudes and concerns about data privacy.

3) App permissions and comfort levels

Delving into specifics, we explored the comfort levels of respondents regarding healthcare apps accessing different types of personal information (e.g., age, gender, health-related data, photos, voice, fingerprint or face recognition, contact list, calendar, and location).

4) Access method preference

We inquired about preferred methods of accessing healthcare apps, such as using a password, biometrics, or both, aiming to discern patterns or preferences in access security and convenience.

5) Data security and encryption concerns

Probing into data security aspects, questions explored areas such as concerns about cloud storage and the importance of data encryption in healthcare apps, allowing us to comprehend the weight respondents place on these aspects.

The survey was designed not only aligns with our fundamental objectives but also embodies a holistic approach towards understanding user perceptions and concerns about privacy and security in mobile health apps. Our survey, while in-depth, was crafted with the utmost consideration for inclusivity, ensuring that questions encompassed a wide array of privacy and security aspects without becoming entwined in technical jargon that might alienate novice users.

Mindful of the fact that lengthy and complex questions could potentially skew responses due to respondent fatigue or disengagement, we strived to maintain a balance. The questions were framed in a manner that they were succinct and straightforward, thereby encouraging genuine and thoughtful responses from participants across various demographic and knowledge spectrums. Thus, our survey sought to be a confluence of depth and simplicity, ensuring robust data collection while respecting the user's experience and knowledge.

B. Phase 2: Collection of End-Users' Responses

In the second phase of our research, spanning from the beginning of September 2023 to the end of October 2023, we dedicated our efforts to the meticulous collection of end-users' responses. With a population nearing 32 million in Saudi Arabia [31], attaining a sample size that could closely mirror this diverse populace was pivotal. A

total of 357 responses were garnered, which might appear minuscule at a mere approximately 0.0011% of the entire population, but nonetheless, provided a substantial and insightful dataset for our analysis.

Intriguingly, when we delve into the mathematical realm of research, the calculated ideal sample size, assuming a confidence level of 95% and a margin of error of 5%, for a population of 32 million is approximately 384. This implies that a meticulously designed survey of 384 individuals, diverse in demographics, could present reliable and generalizable insights about the entire population. Our actual sample size of 357 is remarkably close to this ideal, providing a solid foundation upon which to build our analyses and draw insights that could be applicable to the broader population.

This minimal percentage, while seemingly diminutive, is not to be dismissed. In the realm of research, especially where perceptions and experiences are concerned, even a small segment of the population can provide potent insights and illuminate patterns or trends that are applicable on a larger scale. It's the diversity and quality of responses that hold weight, ensuring that the findings are not skewed or limited to a particular demographic or perspective.

Efforts were distinctly channelled to disseminate the survey across varied demographics, ensuring the inclusion of different ages, occupations, and social strata to derive a holistic insight into the privacy preferences across the healthcare system's user spectrum.

Prior to the primary data collection, a pilot study was conducted with 10 participants. This was crucial to validate the survey's comprehensibility, relevance, and robustness, enabling fine-tuning and minor adjustments to enhance its efficacy and ensure that the subsequent collection of responses was as accurate and reflective of user perceptions as possible.

C. Phase 3: Analyzing Data

For the quantitative data analysis phase of this research, we opted to utilize Python, a programming language renowned for its extensive statistical capabilities and flexibility. This decision enabled us to engage in a comprehensive exploration of the data, employing a multifaceted array of statistical techniques to uncover significant trends and relationships.

1) Descriptive analysis

Descriptive analysis was employed to summarize and delineate the fundamental characteristics of the data in this study. It involved providing succinct summaries about the sample and measurements, including percentages and counts of respondents across different demographic categories such as age, gender, education, and occupation.

2) Correlation analysis

Correlation analysis was utilized to explore the relationships between demographic variables (such as age, gender, education level) and attitudes towards data sharing and privacy concerns. This method facilitated an understanding of how these demographic factors correlate with user preferences and behaviours.

3) Frequency analysis

Frequency analysis was conducted to determine the regularity of participants engaging in specific behaviours, like modifying app permissions. This analysis aided in identifying prevalent behaviours among users and their frequencies.

4) Sentiment analysis

Sentiment analysis was potentially used to measure respondents' feelings towards privacy concerns, data sharing with third parties, and security measures in healthcare apps. Categorizing responses into various sentiment categories, including "Strongly Agree," "Neutral," and "Strongly Disagree," helped in assessing the overall attitudes of users.

5) Cross-tabulation analysis

Cross-tabulation, or contingency table analysis, was likely employed to investigate the relationships between two or more categorical variables. This involved analyzing how different user categories, defined by demographics such as age or education, varied in their survey responses.

6) Trend analysis

Trend analysis was used to observe patterns or tendencies in the survey data across various demographic segments, such as the trend of privacy concerns among different age groups or educational levels.

7) Comparative analysis

Comparative analysis was applied to contrast the responses between disparate groups. This included comparing levels of comfort in sharing various types of data, such as health data versus location data, among users.

Collectively, these types of analysis provided a comprehensive understanding of the survey data, revealing detailed insights into user demographics, behaviours, preferences, and attitudes toward health apps. Each analytical approach contributed significantly to a more profound understanding of the diverse aspects examined in this study.

IV. Result

A. Descriptive Analysis

Table I provides a comprehensive understanding of the demographics of individuals engaging with health apps. One of the standout observations is the dominance of male respondents, accounting for a substantial 81.95%. This could suggest a stronger inclination among men towards health apps or their participation in related surveys.

Examining the age distribution reveals that the 35–44 age group forms the largest segment at 43.79%, followed closely by those aged 18–24 at 36.09%. This prominence of younger to middle-aged individuals could point towards their heightened adaptability to technological solutions. On the contrary, the older age groups, particularly those aged 55–64 and above, are less represented, accounting for just 2.66%.

In terms of educational background, a significant majority, 58.28%, hold a bachelor's degree,

while 18.34% have pursued graduate studies. This data might indicate that those with higher educational qualifications have a greater affinity for health apps. When observing occupations, employed individuals constitute the majority at 58.88%. This suggests that working professionals might find health apps especially beneficial. Students, representing 27.22%, further highlight the interest of younger demographics in health tech solutions. Conversely, the unemployed and retired categories are lesser represented at 10.95% and 2.96%, respectively.

TABLE I. DEMOGRAPHIC BREAKDOWN OF SURVEY RESPONDENTS

Factor	Category	Count	Percentage (%)
Gender	Male	277	82
	Female	61	18
Age	18–24	122	36
	25–34	45	13
	35–44	148	44
	45–54	14	4
	55+	9	3
Occupation	Student	92	27
	Employed Full time	199	59
	Unemployed	37	11
	Retired	10	3
Education	High school and lower	58	18
	Diploma	21	6
	College certificate	197	58
	Postgraduate	62	18
Skill	Novice	12	4
	intermediate	142	42
	Advance	184	54

A scrutiny of mobile skill levels indicates that a dominant 54.44% are advanced users. This might imply that health apps cater more effectively to those with proficient mobile skills or that they are simply more popular among this group. Medium-skilled users aren't far behind at 42.01%, while novice users, making up just 3.55%, perhaps indicate a skill gap in navigating health apps.

In summation, these detailed insights paint a clear picture of the demographic landscape of health app users, offering invaluable insights for developers, marketers, and other stakeholders in the health tech domain.

B. Sentiment Analysis

Fig. 2 reveals participants' sentiments regarding sharing their health data with health app. A predominant sentiment among respondents is a combination of being "Strongly Concerned" and "Concerned", with 47.34% (160 respondents) falling into this category. This suggests a significant level of apprehension about data sharing among the majority of respondents.

However, the spectrum of opinions varies. A notable 28.40% (96 respondents) maintain a 'Somewhat Concerned' stance on the issue, indicating a moderate level of concern. On the other end of the spectrum, 24.26% (82 respondents) are either 'Slightly Concerned' or "Unconcerned", suggesting a less perturbed attitude towards data sharing with advertisers or third parties.

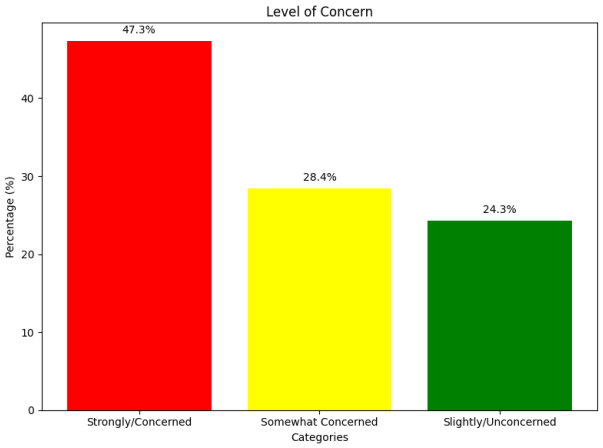

Fig. 2. User concerns when sharing data with health apps (combined categories).

In summary, while a significant proportion of respondents harbor concerns about sharing health data with health apps, there is a varied spectrum of opinions, highlighting the diversity of perspectives on data privacy in the context of health apps.

The analysis of user sentiments towards sharing data with health apps versus sharing data for ads reveals intriguing differences as shown in Fig. 3. In the context of sharing data with health apps, a combined category of "Strongly Concerned" and "Concerned" encompasses 47.34% (160 respondents), indicating a substantial level of apprehension among users. This concern, however, appears to be even more pronounced when it comes to sharing data for advertising purposes, where a combined 73% fall into the "Strongly Concerned" and "Concerned" categories, signaling a heightened concern in this area.

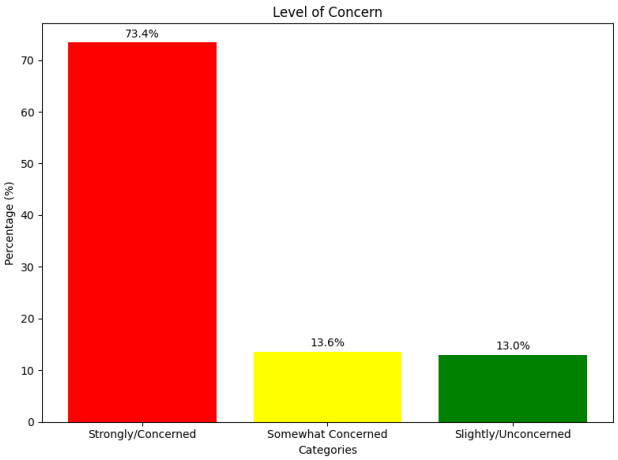

Fig. 3. User concerns when sharing data for advertising purposes.

Comparatively, the sentiment towards sharing data for ads shows a more unified concern. Most users express a stronger hesitation or reluctance to share their health data for advertising purposes. This stark contrast highlights a more acute sensitivity and wariness when it comes to potential commercial use of personal health information.

In essence, while there is a considerable concern among users about sharing data with health apps in

general, the apprehension intensifies significantly when it comes to sharing data for advertisements. This discrepancy underscores the need for a nuanced approach to user privacy and highlights the importance of clear and transparent communication about data usage, especially in contexts involving third parties or commercial interests.

C. Frequency Analysis

From Fig. 4, it's evident that a majority, 65.68% (222 respondents), are aware that it's possible to modify app permissions within health apps. This indicates a general cognizance of app permissions among the participants. In contrast, 34.32% (116 respondents) are unaware of this possibility, suggesting an area where user education might be beneficial.

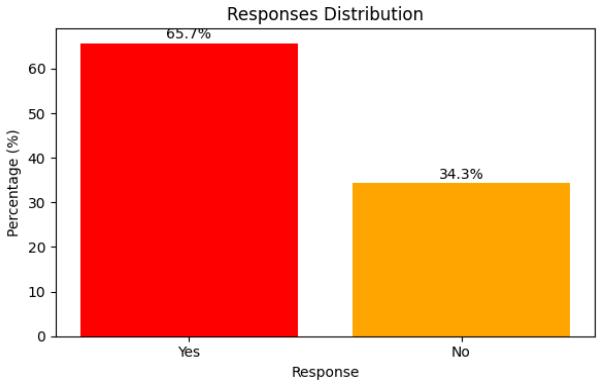

Fig. 4. Awareness of modifying app permissions.

Fig. 5 delves into the frequency with which participants modify these app permissions. The leading trend, represented by 41.72% (141 respondents), is "Rarely", suggesting that even though users might be aware of the feature, they don't frequently utilize it. This is closely followed by "Once in a while" at 40.53% (137 respondents). Interestingly, a considerable 11.54% (39 respondents) mentioned they "Never" modify permissions, while a smaller segment, 6.21% (21 respondents), adjust permissions "Each time they use the health app".

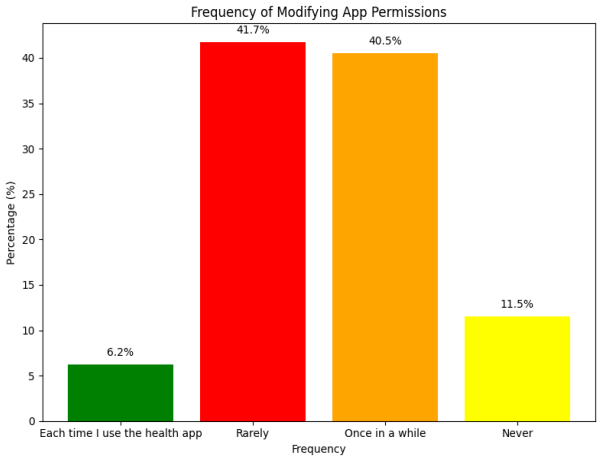

Fig. 5. Frequency of modifying app permissions.

Fig. 6 illustrates individual preferences in sharing different types of data with health apps, categorized into agree, neutral, and disagree responses. Interestingly, the data indicates the highest level of comfort in sharing age and gender information, surpassing even health-related data. This could be attributed to the general perception of these data types as less sensitive or intrusive, and possibly due to their apparent relevance in personalizing health advice and recommendations.

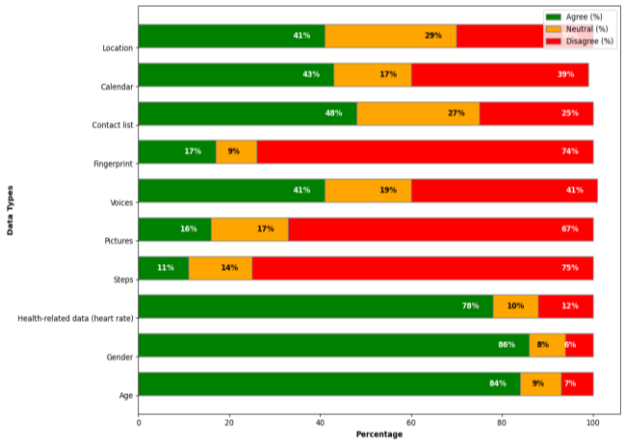

Fig. 6. User preferences for sharing different types of data with health apps.

Although not the highest, there is still a significant willingness to share health-related data (like activity levels and heart rate). This suggests that individuals recognize the importance of these data in health monitoring and improvement, and are relatively comfortable sharing them with health apps.

Data related to fingerprint and face recognition also sees a notable level of agreement. This may indicate a trust in the security of health apps or an understanding of the utility of biometric data in enhancing the personalization of health services.

Contrastingly, data types such as contact lists, calendars, and exact locations show less willingness to be shared, with exact location data, in particular, facing significant disagreement. This highlights strong privacy concerns, especially around location tracking.

Neutral responses are relatively consistent across data types, indicating a segment of the population that is undecided or indifferent about sharing their data with health apps.

When comparing the levels of agreement and disagreement, age and gender data emerge as the most comfortably shared, followed by health-related data. Exact location data is the least preferred for sharing, emphasizing significant privacy concerns.

The data reveals a nuanced view of data sharing preferences with health apps. Individuals appear most willing to share basic demographic information (age and gender), likely due to its perceived non-intrusiveness and relevance. Health-related data also enjoys considerable trust, though concerns around privacy are evident in the reluctance to share more personal and location-based information. These insights could be invaluable for health

app developers in understanding user priorities and apprehensions regarding data sharing.

D. Correlation Analysis

The correlation heatmap in Fig. 7 provides insights into how demographic variables interact with individuals' willingness to share various types of data with a health app. Gender seems to have a minimal impact on data sharing decisions, suggesting no significant differences in preferences based on gender across different types of data like health-related information or fingerprints.

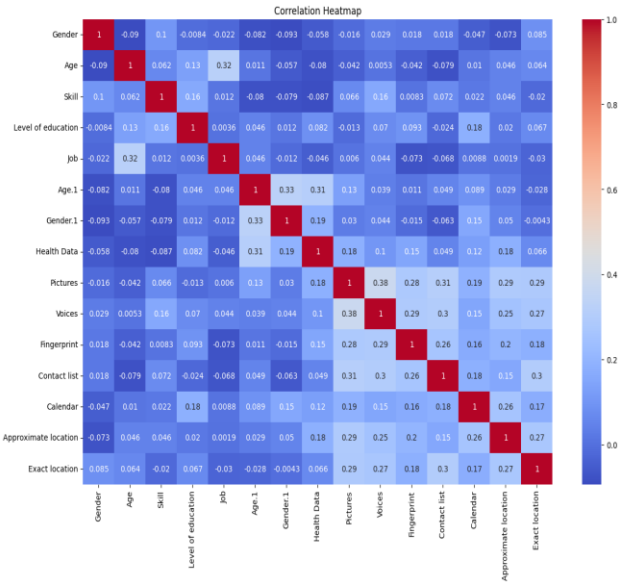

Fig. 7. Correlation heatmap of demographic and data sharing preferences.

When considering age, there is a noticeable correlation with data sharing preferences. This could imply that younger and older age groups have distinct attitudes towards sharing personal data, perhaps due to differing levels of comfort or security concerns. Similarly, an individual's skill level, particularly in digital literacy or technical know-how, correlates with their willingness to share certain types of data. Those with higher skill levels might have heightened awareness about the implications of data sharing.

The level of education also plays a role in shaping data sharing preferences. More educated individuals might exhibit more caution in sharing personal information, possibly owing to a better understanding of privacy and security issues. The nature of one's job also influences data sharing behavior, with variations possibly stemming from the specific demands or privacy norms of different occupations.

Overall, the heatmap suggests that while demographic factors like age and education level significantly influence data sharing behavior, others like gender do not show a strong linear correlation. This indicates that attitudes toward data sharing in health apps are shaped by a complex mix of factors and are not exclusively determined by any single demographic characteristic.

E. Comparative Analysis

The data reveals that nearly half of the respondents' favor using both a password and biometrics for securing their healthcare app, indicating a strong preference for multi-factor authentication. The use of a password only is the second most preferred method, followed by biometrics only. This trend underscores the importance users place on the security of their healthcare apps.

We observe a striking depiction of user concerns regarding cloud storage security in healthcare apps. The chart clearly illustrates that a significant proportion of users exhibit a heightened level of concern. The "Concerned" category, encompassing both "Very Concerned" and "Concerned" responses, represents the most substantial segment, indicating that a majority of users are apprehensive about the security of their health data when stored in the cloud. This finding underscores a critical aspect of user trust and the perceived risks associated with digital health data management.

Conversely, the "Not Concerned" group, which includes both "Not Concerned" and "Not Concerned at All" responses, accounts for a notably smaller portion of the total responses. This disparity suggests that while a segment of users might be more trusting or less aware of potential security issues, the overarching sentiment leans heavily towards caution and concern. The "Neutral" category, indicating a middle ground in opinion, holds a moderate share, reflecting a balanced perspective among a subset of users.

These insights are essential for healthcare app developers and data security professionals. They highlight the need for robust security measures and transparent communication about data handling practices to build user trust and address prevalent security concerns effectively.

The analysis of the responses to the question "How important is encrypting your data in health applications?" reveals the following percentages:

- Important (combining "Very Important" and "Important"): 83.43%
- Neutral: 10.95%
- Not Important (combining "Not Important" and "Not Important at All"): 5.62%

This indicates a strong preference among respondents for the importance of encrypting data in healthcare applications, with a significant majority (over 83%) considering it important. Only a small fraction (approximately 5.62%) perceive it as not important, while around 10.95% remain neutral on this matter.

The willingness of individuals to trade off application performance for enhanced data encryption reveals a varied perspective. A significant portion of the respondents, representing 47.63%, express a clear readiness to accept some reduction in application speed if it means their data is more securely encrypted. This underscores a prioritization of data security over user experience for nearly half of the participants. On the other hand, a substantial 39.05% of respondents display a conditional stance, indicating their decision depends on the extent of the performance sacrifice required. This

group might be weighing the practical implications of slowed performance against the benefits of stronger encryption. Lastly, a smaller yet notable 13.31% of the participants are not in favor of sacrificing application performance, suggesting a preference for maintaining optimal user experience even if it means compromising to some extent on data encryption. These varied responses highlight the differing priorities and concerns individuals have when it comes to balancing security and functionality in healthcare applications.

V. Discussion

Our research, structured into three distinct phases, sought to unravel the complex perceptions users in Saudi Arabia have towards mobile health apps. Guided by three essential research questions, our study focused on understanding privacy preferences, exploring the impact of demographic factors on user engagement, and assessing user preferences regarding access methods and data security. The analysis of our survey responses provided rich insights into these areas.

A. Understanding User Privacy Preferences and Concerns (RQ1)

The survey results highlighted a significant concern among users about sharing health data with external parties. A majority of respondents expressed strong reservations about such data sharing practices. Users were more comfortable sharing basic demographic information, like age and gender, as opposed to more sensitive data like location, which faced considerable resistance. These findings underline a keen awareness and concern for privacy among health app users in Saudi Arabia, emphasizing the necessity for stringent privacy measures and transparent data management.

B. Influence of Demographic Factors on User Engagement and Preferences (RQ2)

The data indicated a crucial need for health apps to align with user preferences, particularly concerning privacy and security. A preference for multi-factor authentication, especially the use of passwords combined with biometrics, was evident. This trend points towards a user tendency to favor strong security measures without sacrificing accessibility. The marked preference for data encryption and the readiness to accept some reduction in app performance for enhanced security underscores the importance of secure data practices in building user trust and engagement.

C. User Preferences Regarding Access Methods and Data Security (RQ3)

The study found that perceptions of security and privacy features significantly influence user trust and engagement with health apps. Concerns about cloud storage security and a strong preference for data encryption were predominant, indicating security's vital role in shaping user trust. The mixed responses towards compromising application performance for better data encryption show a nuanced balance between user experience and security. Users appear willing to tolerate some performance trade-offs for greater data security, highlighting their complex expectations from health apps.

The demographic analysis, particularly the correlation heatmap, shed light on how different factors affect data sharing preferences. Age and education level were significant determinants, with younger and more educated users showing more discernment and caution in sharing personal data. Gender, however, appeared to have a minimal impact, suggesting a universal emphasis on privacy across different genders.

These findings are crucial for developers and policymakers in the health technology sector. The pronounced demand for strong security measures and transparent data practices should inform the design and development of health apps. Aligning these apps with user preferences for privacy and security is essential to fostering trust and promoting broader use. The survey also highlighted the importance of user education, particularly regarding app permissions, pointing to a significant area for further development and policy focus.

VI. Conclusion

This study has provided a comprehensive understanding of user attitudes and preferences towards mobile health apps in Saudi Arabia, revealing nuanced insights into privacy concerns, the influence of demographic factors, and preferences regarding access and security. The research uncovered a significant emphasis on privacy among users, with a majority expressing reservations about sharing health data with third parties. This concern was particularly pronounced in the context of sharing sensitive information like location data, highlighting the paramount importance users place on their privacy.

Demographic factors, such as age and education, emerged as significant influencers in user engagement and preferences, with younger and more educated users displaying a heightened awareness and cautious approach towards sharing personal data. In contrast, gender appeared to have a minimal impact on privacy concerns, indicating a widespread apprehension about data security across different demographics.

The study also revealed a strong user preference for robust security measures in health apps. Features like multi-factor authentication, combining passwords and biometrics, were highly favored, reflecting the users' desire for secure yet accessible health apps. The overwhelming preference for data encryption and the willingness of many users to compromise on app performance for enhanced security underscored the crucial role of robust data protection in building user trust and engagement.

While this study offers valuable insights, it is important to acknowledge its limitations. The sample size, though statistically significant, represents a small fraction of the entire population. Demographic imbalances in the sample may limit the generalizability of the findings, and survey responses may have been influenced by self-reporting biases, including

overestimation or underreporting of privacy concerns. Additionally, certain technological aspects, such as implementing specific data security measures, were outside the scope of this research. Future studies should aim for larger, more diverse samples across different regions, age groups, and socio-economic backgrounds. Cross-validation with observational or system-logged data could improve the reliability of findings, while qualitative research could provide deeper insights into user motivations and concerns. Further exploration of technical evaluations of security protocols within mHealth apps is also recommended.

In summary, this research contributes valuable insights into the complex dynamics of health app usage, underscoring the critical need for privacy, security, and user-centric design in the evolving domain of health technology. As the adoption of health apps continues to expand, addressing limitations and advancing future research will be pivotal in shaping solutions that not only meet technological standards but also resonate with the needs and concerns of end-users.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

AA was responsible for conceptualization, methodology, writing—original draft preparation, and writing—review and editing; JOA contributed to validation, resources, supervision, project administration, and writing—review and editing; KAA performed data curation, software, methodology, writing—review and editing, and supervision; all authors approved the final version of the manuscript.

REFERENCES

[1] A. Papageorgiou, M. Strigkos, E. Politou *et al*., "Security and privacy analysis of mobile health applications: The alarming state of practice," *IEEE Access*, vol. 6, pp. 9390–9403, Jan. 2018.

[2] D. Kotz, C. A Gunter, S. Kumar *et al*., "Privacy and security in mobile health: A research agenda," *Computer*, vol. 49, no. 6, pp. 22–30, Jun. 2016.

[3] F. Zubaydi, A. Saleh, F. Aloul *et al*., "Security of mobile health (mHealth) systems," in *Proc. IEEE 15th Int. Conf. on Bioinformatics and Bioengineering (BIBE)*, 2015, pp. 1–5.

[4] K. Knorr and D. Aspinall, "Security testing for Android mHealth apps," in *Proc. IEEE 8th Int. Conf. on Software Testing, Verification, and Validation Workshops (ICSTW)*, 2015, pp. 1–4.

[5] Medical Technology—Worldwide. [Online]. Available: https://www.statista.com/outlook/hmo/medical-technology/worldwide

[6] Healthcare IT Market (Type: Healthcare Provider Solutions, Healthcare Payer Solutions, and HCIT Outsourcing Services), and (End User: Healthcare Providers and Healthcare Payers)—Global Industry Analysis, Size, Share, Growth, Trends, Regional Outlook, and Forecast 2023–2032. [Online]. Available: https://precedenceresearch.com/healthcare-it-market

[7] MedTech Europe. (2023). The European Medical Technology Industry in Figures 2023. [Online]. Available: https://www.medtecheurope.org/wp-content/uploads/2023/10/the-european-medical-technology-industry-in-figures_2023.pdf

[8] 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, no. 1, pp. 1–8, Jan. 2015.

[9] B. Qudah and K. Luetsch, "The influence of mobile health applications on patient-healthcare provider relationships: a systematic, narrative review," *Patient Education and Counseling*, vol. 102, no. 6, pp. 1080–1089, Jun. 2019.

[10] T. Mabo, B. Swar, and S. Aghili, "A vulnerability study of mHealth Chronic Disease Management (CDM) applications (apps)," in *Trends and Advances in Information Systems and Technologies: Volume 1*, Springer International Publishing, 2018, pp. 1–10.

[11] M. Hussain, A. A. Zaidan, B. B. Zidan *et al*., "Conceptual framework for the security of mobile health applications on android platform," *Telematics and Informatics*, vol. 35, no. 5, pp. 1335–1354, Aug. 2018.

[12] R. Adhikari, D. Richards, and K. Scott, "Security and privacy issues related to the use of mobile health apps," in *Proc. ACIS*, 2014, pp. 1–10.

[13] S. Gejibo, F. Mancini, K. A. Mughal *et al*., "Secure data storage for mobile data collection systems," in *Proc. Int. Conf. on Management of Emergent Digital EcoSystems*, 2012, pp. 1–5.

[14] M. Chowdhury, M. Ferdous, and R. Biswas, "Privacy-aware mobile health monitoring: Current trends and challenges," *Health Informatics Journal*, vol. 25, no. 3, pp. 607–622, 2019

[15] E. P. Morera, I. de la T. Díez, B. Garcia-Zapirain *et al*., "Security recommendations for mHealth apps: Elaboration of a developer's guide," *Journal of Medical Systems*, vol. 40, no. 1, pp. 1–13, May 2016.

[16] B. Mesko, "Future directions of digital health," *Digital Health: Scaling Healthcare to the World*, pp. 339–363, Jan. 2018.

[17] B. Stack. Here's how much your personal information is selling for on the dark web. [Online]. Available: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

[18] S. P. Cohn, "Privacy and confidentiality in the nationwide health information network," *National Committee on Vital and Health Statistics*, 2006.

[19] B. Aljedaani, A. Ahmad, M. Zahedi *et al*., "An empirical study on developing secure mobile health apps: The developers' perspective," in *Proc. IEEE Asia-Pacific Software Engineering Conf. (APSEC)*, 2020, pp. 1–10.

[20] L. H. Iwaya, A. Ahmad, and M. A. Babar, "Security and privacy for mHealth and uHealth systems: A systematic mapping study," *IEEE Access*, vol. 8, pp. 150081–150112, Dec. 2020.

[21] V. Stephani, D. Opoku, and W. Quentin, "A systematic review of randomized controlled trials of mHealth interventions against non-communicable diseases in developing countries: Lessons learned," *BMC Public Health*, vol. 16, no. 1, 572, 2016. doi: 10.1186/s12889-016-3226-3

[22] S. Kumar and A. Smith, "mHealth applications during COVID-19: A global perspective," *Global Health Journal*, vol. 25, no. 3, pp. 199–212, 2020.

[23] S. Lee and J. Park, "Data breaches in mHealth: Insights from real-world incidents," *Cybersecurity and Health*, vol. 28, no. 2, pp. 150–173, 2021.

[24] R. Johnson, L. Smith, and T. Kim, "Enhancing data security in mHealth applications: A review of encryption protocols," *Health Tech Review*, vol. 30, no. 4, pp. 210–234, 2022.

[25] R. Lopez and M. Torres, "Enhancing user experience in mHealth through multilingual support," *Int. J. Health Tech*., vol. 18, no. 3, pp. 88–112, 2020.

[26] Y. Chen, J. Lee, and H. Wang, "Predictive analytics in mHealth applications using machine learning: A systematic review," *Journal of Medical Informatics*, vol. 45, no. 2, pp. 123–145, Oct. 2022.

[27] V. Patel, B. Jones, and N. Singh, "Blockchain in healthcare: Securing data through decentralized systems," *Health Informatics Advances*, vol. 35, no. 2, pp. 156–180, 2021.

[28] M. Plachkinova, S. Andrés, and S. Chatterjee, "A taxonomy of mHealth apps—Security and privacy concerns," in *Proc. 48th Hawaii Int. Conf. on System Sciences (HICSS)*, 2015, pp. 1–10.

[29] L. Parker, V. Halter, T. Karliychuk *et al*., "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, May–Jun. 2019.

[30] T. Schroeder, M. Haug, and H. Gewald, "Data privacy concerns using mHealth apps and smart speakers: Comparative interview study among mature adults," *JMIR Formative Research*, vol. 6, no. 6, e28025, Jun. 2022.
[31] L. Zhou and B. Parmanto, "User preferences for privacy protection methods in mobile health apps: A mixed-methods study," *International Journal of Telerehabilitation*, vol. 12, no. 2, pp. 13–26, Dec. 2020.
[32] Y. Dang, S. Guo, X. Guo *et al*., "Privacy concerns about health information disclosure in mobile health: Questionnaire study investigating the moderation effect of social support," *JMIR mHealth and uHealth*, vol. 9, no. 2, e19594, Feb. 2021.
[33] M. Plachkinova, S. Andrés, and S. Chatterjee, "A taxonomy of mHealth apps: Security and privacy concerns," in *Proc. 48th Hawaii Int. Conf. on System Sciences (HICSS)*, IEEE, 2015, pp. 1–10.
[34] S. Jusoh, "A survey on trend, opportunities, and challenges of mHealth apps," *Int. J. Interact. Mob. Technol*., vol. 11, no. 6, pp. 73–85, Nov. 2017.
[35] A. Ferreira, J. Muchagata, P. Vieira-Marques *et al*., "Perceptions of security and privacy in mHealth," in *Proc. Int. Conf. on Human-Computer Interaction*, Cham: Springer International Publishing, 2021, pp. 1–10.
[36] A. A. Atienza, C. Zarcadoolas, W. Vaughon *et al*., "Consumer attitudes and perceptions on mHealth privacy and security: Findings from a mixed-methods study," *Journal of Health Communication*, vol. 20, no. 6, pp. 673–679, Apr. 2015.
[37] P. Krebs and D. T. Duncan, "Health app use among US mobile phone owners: A national survey," *JMIR mHealth and uHealth*, vol. 3, no. 4, e4924, Nov. 2015.
[38] General authority for statistics. [Online]. Available: htttp://www.stats.gov.sa/
[39] P. Davis and R. Martin, "Navigating HIPAA compliance in digital health technologies," *Health Policy Journal*, vol. 39, no. 1, pp. 55–67, 2020.
[40] K. Müller and G. Becker, "GDPR compliance challenges in mHealth applications," *Journal of Legal and Regulatory Studies*, vol. 22, no. 1, pp. 67–90, 2021.