European Journal of Information Technologies and Computer Science
Vol 4 | Issue 3 | August 2024
ISSN 2736-5492

RESEARCH ARTICLE

Usability, Reliability, Security, and Status: Unpacking the Factors Shaping User Choice between iOS and Android in Saudi Arabia

Abdullah Abdualrahman H. Alzahrani*

ABSTRACT

This investigation delves into user perceptions of iOS and Android operating systems within the Kingdom of Saudi Arabia. A sample of 594 participants was recruited to explore their preferences concerning usability, reliability, security, social influence, and prior experiences with both systems. The study reveals a modest predilection for iOS in terms of user-friendliness and perceived information security. Interestingly, a counterintuitive finding emerged: Android users, particularly females, exhibited high confidence in information security despite encountering a greater number of cyberattacks. Additionally, the research highlights the influence of sociodemographic factors, such as age, education level, and gender, on system selection. A pronounced desire to utilize iOS was observed among younger users, females, and individuals with higher educational attainment. While the study provides a robust foundation for understanding user preferences within the Saudi Arabian context, limitations such as sample size and geographic focus necessitate further research efforts across more heterogeneous populations to achieve a more generalizable depiction.

Submitted: July 07, 2024

Published: August 18, 2024

10.24018/ejcompute.2024.4.3.130

Departments of Computers, Engineering and Computers College, Alqunfuda Umm Al Qura University, Saudi Arabia.

***Corresponding Author:**
e-mail: aahzahrani@uqu.edu.sa

Keywords: Android, iOS, Software Quality, User perception.

1. Introduction

Mobile operating systems, like iOS and Android, have become ubiquitous tools shaping our daily lives. Understanding user perceptions of these systems is crucial for software developers to create user-centric experiences. Usability, reliability, and security are the holy trinity of quality attributes of software systems. Usability can be considered to be the extent of ease and enjoyment of using the program or software system, and reliability reflects the extent to which the program's performance remains consistent as expected and does not fail or become unresponsive. Finally, the software system or program must have a degree of security that makes the user feel that his data and access to his devices are protected from harm [1]–[5].

This study aims to investigate the extent of these three qualities or quality features (usability, reliability, and security) in Android systems, which operate on many phone devices such as Samsung phones, and iOS systems, which operate on iPhone devices, and compare these features and measure their impact with other factors in users' choices.

In addition, this study investigates user preferences for iOS and Android operating systems in Saudi Arabia, focusing on factors influencing user choice, including usability, reliability, security perceptions, social influence, and prior experiences. The study aims to identify potential disparities in user experiences and shed light on the interplay between these factors in shaping user preferences.

This research paper commences by outlining the research questions that guided the investigation. Subsequently, it delves into the methodological approach employed to address these questions. To establish a robust theoretical framework, the paper explores the pertinent scientific background and existing literature relevant to the topic. The empirical findings of the study are then meticulously presented and analyzed. Finally, the paper culminates with a discussion of the conclusions drawn from the research, acknowledging any limitations inherent to the study design.

2. Research Questions

This research aims to investigate the choices of individuals between two well-known systems, iOS and Android. The investigation of the choices relies on the impacts of

the Holy Trinity of Software Quality (Usability, Reliability, and Security) and the other factors that are related to the users (Age, Educational Level, Gender, social outlook, and previous experience with rival systems). Therefore, two research questions were formulated in this research:

- *RQ1: Do usability, reliability, and security concerns impact the choice of individuals in Saudi Arabia between iOS and Android?*

In order to answer this question, a number of widely known tests can be employed, and a few related questions will be provided to participants to allow them to draw a complete conclusion.

- *RQ2: Do Age, Educational Level, Gender, social outlook, and previous experience with rival system impact the choice of individuals in Saudi Arabia between iOS and Android?*

To answer these questions, the participants will be asked to share their information on gender, age, and educational level. This information will be provided anonymously. However, to investigate the previous experience with rival systems, the individuals will be provided with appropriate questions to rate their experience, and then the collected data will be analyzed with other collected data. Moreover, to investigate social outlook, the individuals will be provided with questions to express their preference on the appearance with what product (iOS or Android) in social gatherings.

3. Methodology

In this research, the employed methodology is a survey that combines a set of tests and questions in order to collect the required data to analyze for the sake of answering the aforementioned research questions. Tables II–IV in Appendix contains all the questions that were presented in the questionnaire.

The questionnaire consists of four main sections. The first section explains the purpose of the ongoing research, assures participants that the research is for scientific purposes only, and obtains their consent to participate. Moreover, they are assured that they can also refuse and leave at any time they wish.

In the second part of the questionnaire, personal information such as age, education level, and gender will be requested. In addition, they will be asked what type of device they are using now, whether it is iOS or Android. Finally, they will be asked what device they prefer to appear on at social gatherings.

As for the third part of the questionnaire, based on their answer in the first part about the device they are currently using, whether it is Android or iOS, SUS [6] test will be presented to them. This test allows users to measure the usability and satisfaction of their current devices. SUS [6] is a test established by Brooke and is used to assess the usability of systems, website phones etc., and provides a results out of 100 points.

In addition, a question established by Bangor *et al.* [7], which is a 7-point adjective scale (1–Worst Imaginable, 2–Awful, 3–Poor, 4–OK, 5–Good, 6–Excellent, 7–Best Imaginable), will be used to give meaning to the results of the SUS test. Furthermore, the loyalty of individuals to the systems will be assessed by Reichheld *et al*. [8]–[10] 11-point likelihood recommend question.

In the last part of the questionnaire, participants will be asked about their previous experience with the rival device or system, whether it is iOS or Android, depending on their answers about their current device. This question will rate their previous experience and will be a 5-point question from 0 to 4, where 0 is considered a very unsatisfactory experience, and 4 is considered a very satisfactory experience. In addition, there will be a "not applicable" choice if they have no previous experience with the rival system.

In addition, and in order to validate the participants' attachment to the operating system or the device itself, participants will be asked if the operating system on their current devices has changed and whether they will continue to like it and use it or not. This question will be closed with a yes or no answer.

Finally, in this part of the survey, the questions will be to assess the reliability and security that participants feel with their current devices and operation systems. Participants will be asked to rate how reliable and secure their operating system, whether iOS or Android, based on their answers in the first part of the survey. The rating they provide will be from 0 to 4, where 0 means "strongly disagree", and 4 means "strongly agree". In addition, to further assess the security they feel, they will be asked about how easy and fast the recovery is after any cyber-attack on their current devices. The rating will be from 0 to 0, where 0 represents strongly disagree, and 4 represents strongly agree. There will be an additional option, "not applicable," if they have not been exposed to any cyber-attack.

This questionnaire was designed using Google Forms, which enables us to create questionnaire forms to collect data through electronic forms. After designing the electronic questionnaire, it was sent to the target group via emails and social media. The target group was iOS or Android users in the Kingdom of Saudi Arabia.

The questionnaire was sent to 800 participants, and a total of 594 participants responded, with a response rate of approximately 74%. In Fig. 1a, the distribution of participants according to gender is shown, as 88% of the participants are males and 12% of the participants are females.

In addition, the distribution of participants according to age groups is shown in Fig. 1b. As it appears, about 47% of the participants are from the age group of 35 to 44 years. The age group from 45 years to 54 years appears in second place, with a percentage of 27% of the participants. Finally, Fig. 1c shows the distribution of participants according to their level of education. There are four levels, and the highest percentage of participants are those who hold above bachelor's degree at a rate of 58% of the participants. In addition, the participants who hold a bachelor's degree occupy the second place, at a rate of 34% of the total participants.

4. Related Work and Background

Mobile phone operating systems are among the most widely used systems nowadays. In fact, these systems are a group of programs that allow us to control the features

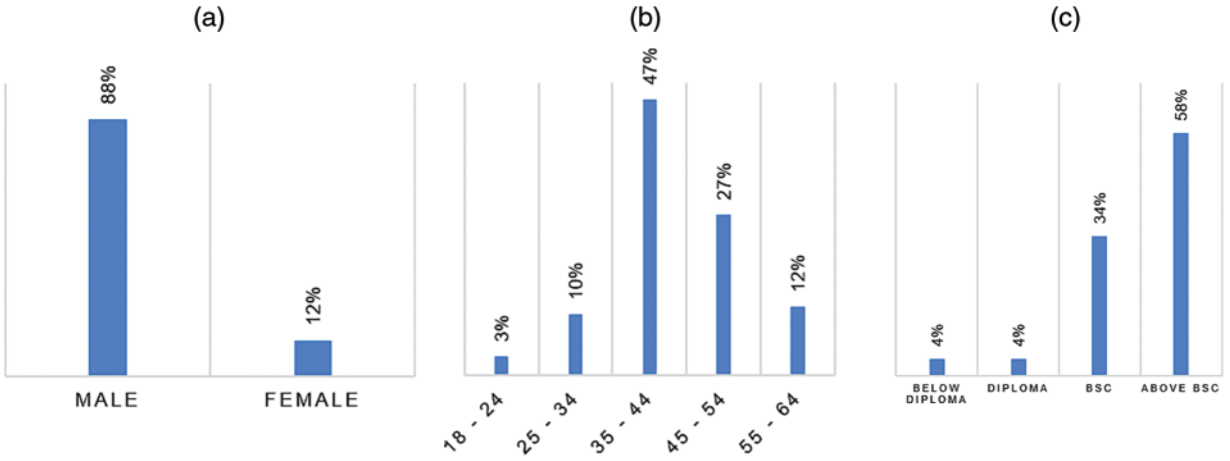

Fig. 1. Distributions of participants by: (a) gender, (b) age group, and (c) education level.

of these devices that we deal with on a daily basis. iOS is developed by Apple and is an operating system that runs on iPhone, iPad, and most Apple products and devices. In addition, Android was developed by Google and is considered an operating system that runs on many mobile devices and tablets, such as Samsung, Huawei, and others [11]–[17].

When these two systems are viewed as software systems, Software system engineering is concerned with developing, maintaining, and testing the quality of these systems. This is accomplished through a set of systematic operations that give an engineering nature to this matter [18], [19].

In addition, software systems engineering details the quality characteristics of systems, and there are many quality attributes, including usability, reliability, and other attributes. Quality attributes can be considered as the measurable and testable features of software systems that lead to a degree of user satisfaction and fulfillment of requirements [5], [20], [21].

Moreover, to validate the software quality attributes, the term software quality assurance (SQA) is coined. SQA is a term in general that expresses the group of processes and activities that are practiced during the systems engineering process to ensure the achievement of certain quality attributes that lead us to user satisfaction and fulfillment of requirements. It is worth noting that Usability, reliability, and security are the holy trinity of quality attributes of software systems [22], [23].

Usability is the most important attribute of systems quality, which is concerned with and centers around the user. Most of the usability checks are in acceptance tests for the system and measure the extent of customer satisfaction with navigation and, generally, user experience with the system. In addition, there are many standardized usability tests [19], [24]. Furthermore, reliability is one of the most critical attributes of software. In addition, reliability can be viewed as an attribute of quality, which expresses the ability of the software system to perform tasks under certain conditions without failure [5], [19], [25]. Moreover, Security is an essential quality attribute in any software system, which is that the system has the ability to protect user data and access to this data [26].

One of the most important factors in measuring software quality and quality assurance is user perception. In addition, there are factors that affect the perception of a user, such as age, gender, culture, and many other factors. Therefore, these factors that affect the user's perception must be taken into account when assessing the quality of software systems [27]–[30].

Oh *et al.* [31] suggested the best practices for users of Android systems, iOS systems, and other systems. The proposed guide is for the purpose of assuring security when using these systems, considering the differences between them in the problems they might be exposed to and the structural nature of these systems.

Ahmad *et al.* [32] conducted a study comparing Android system and iOS in matters of security, and among these issues are the issues of encryption, storage, and sandboxing. The study is considered informative; however, it may be an incentive to conduct a more detailed and systemic investigation that can allow generalization of the study results.

Pieterse *et al*. [33] proposed a new framework to identify modified data for the purpose of analyzing cyber-crimes. The authors in this research focused on user data manipulation in iOS and Android. The authors concluded their results by describing their proposed framework as an assistance to detect modified data for forensic reasons.

Götz *et al*. [34] conducted a huge global study of more than 3,000 participants for the purpose of comparing the personal characteristics of users of a number of systems, including Android and iOS. One of the most important results that emerged in this study was that there are no significant differences between users of iOS system and Android system in terms of personal characteristics and other characteristics that were considered.

Adekotujo *et al*. [35] have conducted a qualitative investigation of a number of research for the purpose of comparing a number of operating systems, including Android system and iOS system. The study was not mainly devoted to the quality attributes of these systems but rather a general comparison. One of the most important results of this study was that the Android system and Windows system are more widespread and popular than iOS system.

Hu *et al*. [36] conducted a study on a number of participants from the age group of 22 to 25 years in order to study the differences in the functions in iOS system and the Android system. In addition, the authors ran a t-test to

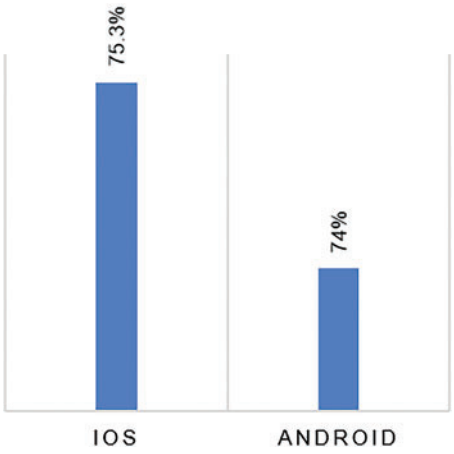

Fig. 2. Comparison of SUS results between Android and iOS.

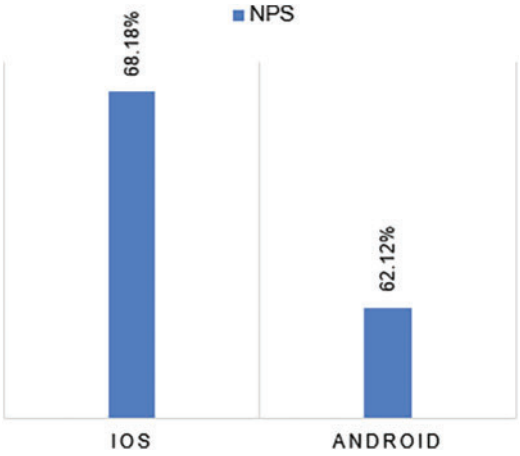

Fig. 3. NET promoter score.

analyze the results. One of the most significant results of this study is that there are no differences in the brand image between the two systems, Android and iOS; however, iOS system is distinguished by the fullness of its brand image, and Android system is distinguished by the strength of its applicability.

Al-Qershi *et al*. [37] conducted an in-depth comparison study between the security in Android system and iOS system for the purpose of answering the always-asked question: Which two systems are more secure? The authors focused mainly on the most famous attacks against Android and iOS.

There are many studies [38]–[47] that have dealt with the comparison between Android systems and iOS systems in several fields. However, most of these studies address the issue of comparison from either security or reliability aspects. In addition, the comparisons are often made either by experimenting with certain features or by analyzing the features and characteristics as discussed in other studies or by developers of these systems.

5. Results and Discussion

In this section, the results of this research will be presented and explained. The results in this research have been divided into two main sections. In the first section, the results of the usability, reliability, and security concerns will be presented and discussed. In the second section, the results of other factors, such as previous experiences with rival systems and social outlook, will be presented and discussed and linked to the information of the participants (age, gender, and level of education).

5.1. *Usability, Reliability, and Security Concerns*

5.1.1. *Usability Concerns*

SUS tests were used to evaluate usability. In addition, SUS tests were conducted for both Android and iOS users. As shown in Table I and Fig. 2, iOS system was rated with a score of 75% by its users, with Excellent Acceptability, and graded A+. On the other hand, Android system obtained, from its users, an assessment score of 74% in SUS test, with Excellent Acceptability and graded A+.

In addition, Fig. 3 indicates a comparison between iOS and Android users in promoting the systems they use. Fig. 3 indicates that the majority of users tend to promote the systems they use, however, iOS users are the slightly more promoting this system at a rate of 68%.

Furthermore, for the purposes of usability assessment, the participants were asked to provide a response to 7-point adjective scale for the system they use. As can be seen in Fig. 4, 49% of iOS users rated their experience with this system as excellent or best imaginable. On the other hand, at a similar rate, about 42% of Android users described their experience with the same description (excellent or best imaginable) of the system they use, which is Android.

In conclusion, it can be alleged that the usability results between iOS system and Android system by their users are adjacent, with a slight superiority for the iOS system in terms of SUS tests scores of usability, in terms of promoting this system by its users, and in terms of describing the users' experience.

5.2. *Reliability Concerns*

Participants were asked whether they agree that the system they are currently using, whether Android or iOS, is a reliable system. In Fig. 5, an opinion poll of iOS users' opinions by gender is shown. As shown in Fig. 5, most users of iOS system, whether males or females, agree or strongly agree that the system is reliable.

On the other hand, as Fig. 6 indicates, the majority of females users of Android system, at a rate of approximately 81%, strongly agree that Android system is reliable, while approximately half of the male users of Android system strongly agree that it is reliable, and the other half agree that it is reliable.

In conclusion, it appears from the surveys of participants' opinions, whether they are Android users or iOS users, that they largely agree that the systems they use are reliable systems and they feel confident in their use of these systems. Therefore, there is no actual difference in the extent to which users of the two systems, whether iOS or Android, feel about its reliability.

TABLE I: SUS Test Score and Interpretations

System	SUS score	Acceptability	Grade
iOS	75.3%	Excellent	A+
Android	74%	Excellent	A+

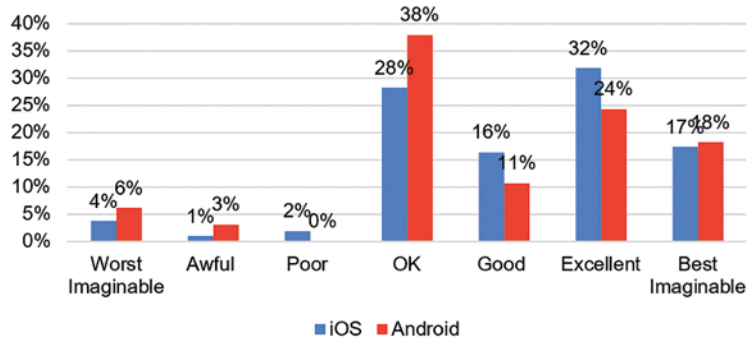

Fig. 4. Adjectives comparison between iOS and Android.

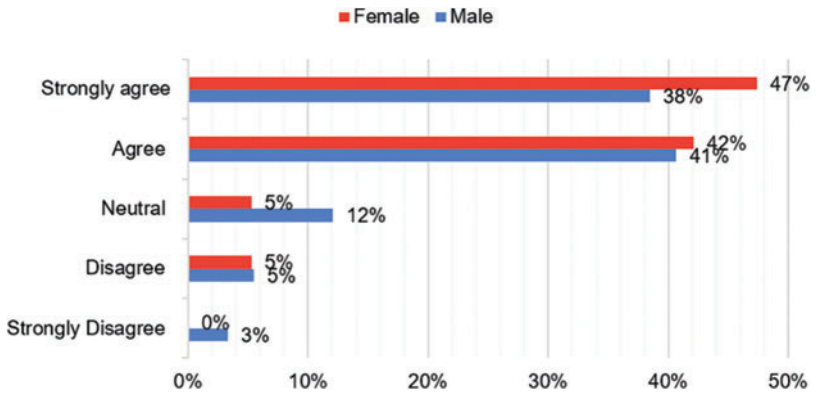

Fig. 5. iOS participants' opinion of the system reliability by gender.

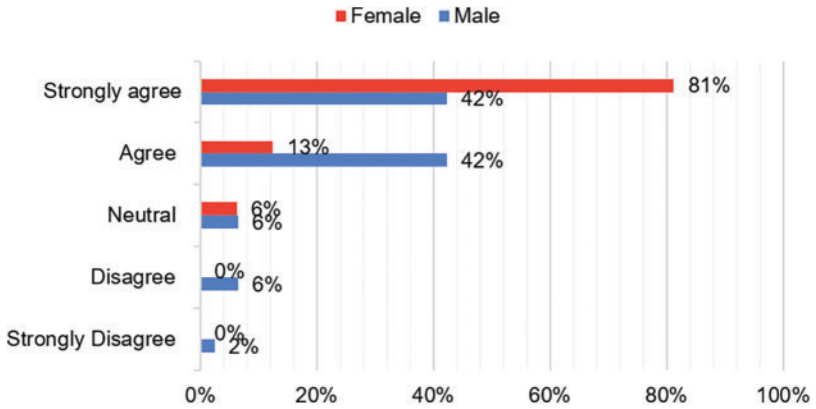

Fig. 6. Android participants' opinion of the system reliability by gender.

5.3. *Security Concerns*

In view of the concerns of security in the two systems, whether iOS or Android, from the point of view of its users, the participants were asked about that. First, they were asked whether they agree that these systems that they use are secure or not, and then they were asked whether they agree on the easiness and rapidness of recovery processes from any cyber-attack they were exposed to, if that occurs.

Fig. 7 illustrates a survey of participants' opinions among iOS system users. As is clearly evident, iOS system users, males and females, participating in this survey, agree or strongly agree that the system is secure, at a rate of 69% and 74%, respectively. On the other hand, less than 11% of males and females who use iOS system disagree or strongly disagree that the system is secure.

As for Android system and the opinions of its users regarding whether the system is secure or not, Fig. 8 displays the results of their opinion poll. As is clearly evident that the female users of Android system, all of these participants agree or strongly agree that the system is secure. However, on the other hand, 63% of male users of Android system agree and strongly agree regarding the system's security, and a significant portion of about 24% of male users of the Android system are neutral.

To further investigate the extent to which users of Android and iOS systems sense security, participants were asked to rate their experiences with exposure to cyber-attacks and the easiness and rapidness of recovery processes from these attacks with these systems. In addition, the results were divided according to gender.

Fig. 9 indicates that around or less than 18% of iOS users participants, whether male or female, have not been exposed to cyber-attacks. However, in contrast, among the participants who use iOS system, 37% of females remain neutral about easiness and rapidness of recovery processes from the cyber-attacks they were exposed to. In addition,

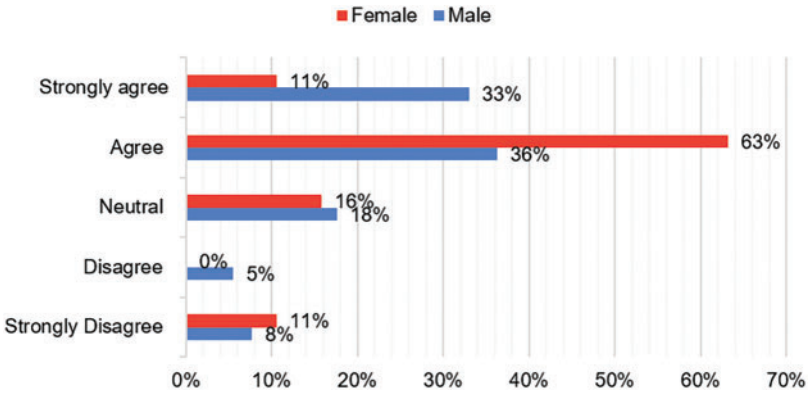

Fig. 7. iOS participants' opinion of the system security by gender.

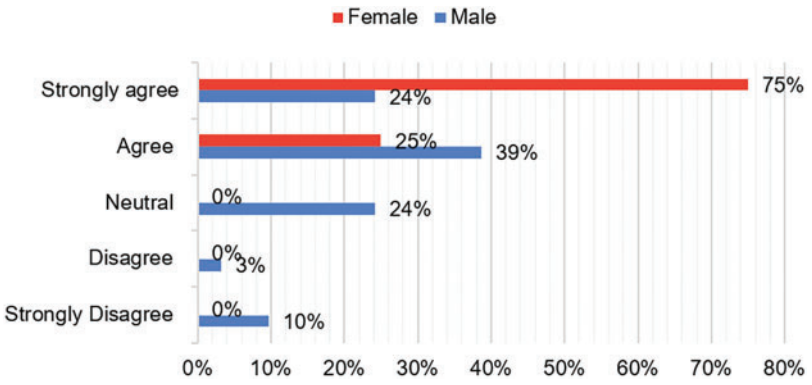

Fig. 8. Android participants' opinion of the system security by gender.

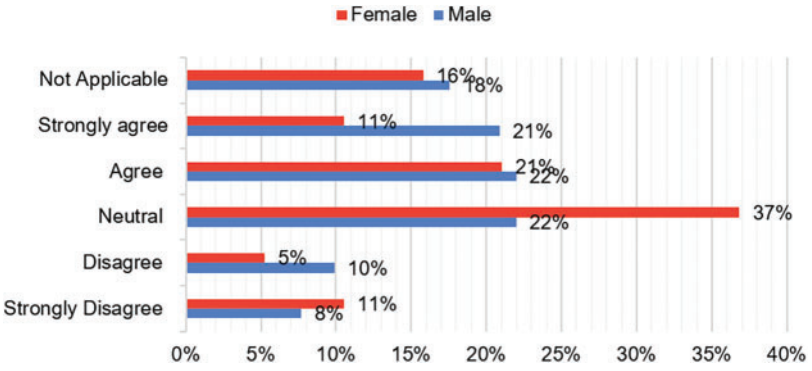

Fig. 9. iOS participants' opinion of how fast and easy to recovery after a cyber incident by gender.

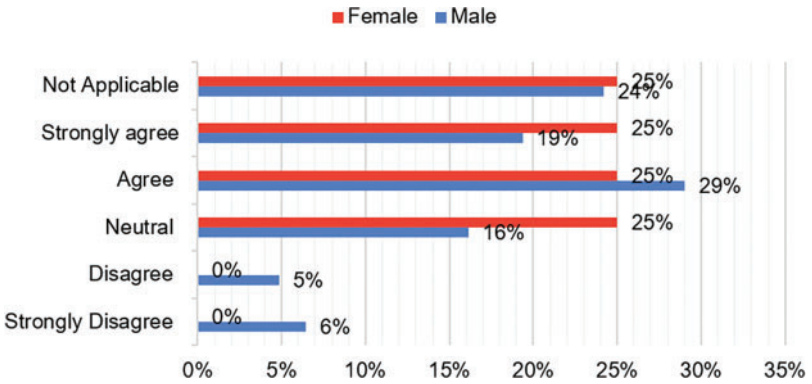

Fig. 10. Android participants' opinion of how fast and easy to recovery after a cyber incident by gender.

22% of iOS male users who were exposed to a cyber-attack also remain neutral with this regard.

On the other hand, as illustrated in Fig. 10, around 50% of male and female participants who use Android systems agree or strongly agree that on easiness and rapidness of recovery processes from the cyber-attacks which they were exposed to. This is worth noting as around 25% of male and female participants who use Android have indicated that they have not experienced cyber-attacks. Moreover, it is important to point out that around 25% of the female participants and 16% of the male participants of users of Android system remain neutral with this regard.

In conclusion, it can be summarized that the majority of participants who use iOS systems believe that their information is secure. As for participants who use Android systems, especially females, they have very high confidence in the security of their information, unlike male participants who use Android systems, about 60% of whom are confident that their information is secure. In addition, it must be noted that the previous results demonstrate that participants who use Android systems have been exposed to cyber-attacks more than participants who use iOS systems.

6. Other Factors

6.1. *Previous Experience*

In order to study the factors affecting individuals' choice between Android and iOS systems, it is worth considering their previous experiences with these systems. For this reason, the participants were asked to rate their previous experiences with the systems. Fig. 11 indicates the responses of the participants who are users of the iOS system regarding their previous experiences with Android systems. The question was an evaluation of their previous experience from 0, which means very unsatisfactory, to 4, Which means very satisfactory, and there is an option as "not applicable" if it does not apply or there is no previous experience with Android system.

As shown in Fig. 11, 58% of the female participants who use iOS system had previous satisfactory or very satisfactory experiences with Android system. In addition, 44% of male iOS users had had a satisfactory or very satisfactory previous experience with Android system. It is worth noting that around 22% of the male participants who use the iOS system had no previous experience with the Android system.

Fig. 12 shows that, on the other hand, considering the participants who are users of the Android system, around 25% of them had no previous experience with the iOS system. However, 31% of male participants describe their previous experience with iOS as satisfactory or very satisfactory, and 23% remain neutral. Although 50% of the female participants who use Android system are neutral regarding their previous experiences with iOS system, 25% of them describe their previous experiences with iOS system as unsatisfactory.

In conclusion, the results of previous experiences can be summarized by expressing that a significant percentage of

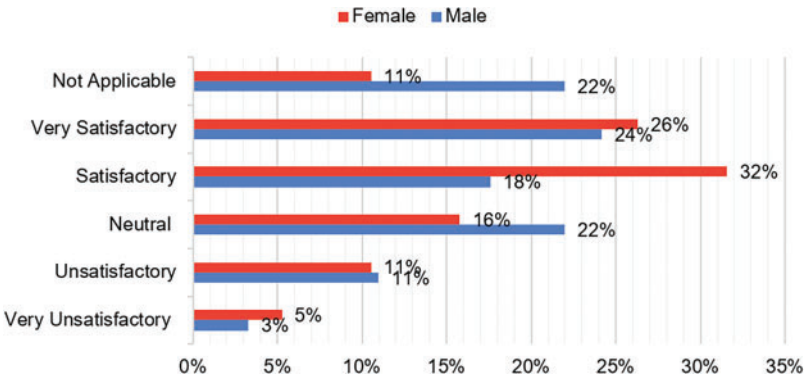

Fig. 11. Evaluation of iOS users of their previous experience with the Android system.

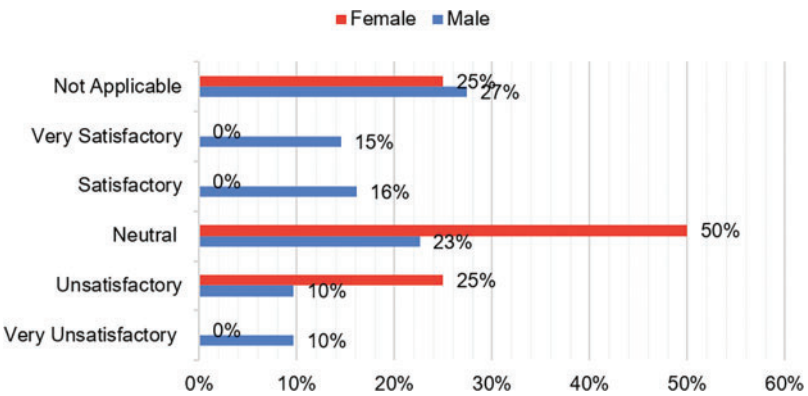

Fig. 12. Evaluation of Android users of their previous experience with the system iOS.

iOS system users have previous experience with Android system, and their experiences are generally satisfactory. On the other hand, participants who use Android, about 25% of whom had no previous experience with iOS system, in addition to, those who had previous experience, especially the female participants who are users of Android system, are neutral or have unsatisfactory experiences with iOS system.

6.2. Social Outlook (Gender, Age, and Educational Level)

The participants were asked whether there had been a change in the current operating system to the rival operating system and whether this would affect the continued use of their devices or not. Fig. 13(a) shows the results of the responses of participants who use iOS system. As is evident from Fig. 13(a), 53% of female participants believe that this affects their continued use of their devices, and this shows a connection from the point of view of female participants who use iOS system to the operating system. On the other hand, 64% of the male participants who use iOS system believe that this has no effect, which shows their attachment to the device and not the operating system.

On the other hand, it can be seen in Fig. 13(b), which shows the responses of participants who use Android system regarding whether the system was changed to iOS system and the extent of this impact on their continued use of their current devices, Fig. 13(b) shows with a percentage exceeding 66% of their responses that this would not affect continued use of their current devices. This might mean that they have attachment to the device and not the operating system.

Fig. 14 demonstrate the responses of participants who use the Android and iOS systems regarding the societal perception of the devices they acquire, whether they have a device that runs iOS or Android system, and what their tendency to appear within social gatherings is. Fig. 14(a) illustrates that approximately 84% of the female participants tend to appear with an iOS device; however, for the male participants, 43% of them have the same tendency.

When considering the age groups, as can be seen in Fig. 14(b), it seems that all age groups from 18 years to 54 years tend to appear on an iOS device, except for one age group, which is the group from 55 years to 64 years, who tend to appear on this Android device. It is worth noting here that the age group from 18 to 24 years is the highest among the groups in the desire to appear with an iOS device.

When considering the level of education, as can be clear in Fig. 14(c), participants who hold a bachelor's degree or above have a higher desire to appear with iOS devices. On the other hand, participants who have a diploma level of education or less have a higher desire to appear for Android devices.

In conclusion, the results of the participants' responses in the questionnaire regarding the societal outlook and the factors of age, education, and gender can be summarized as that the societal outlook is an influential factor in choosing

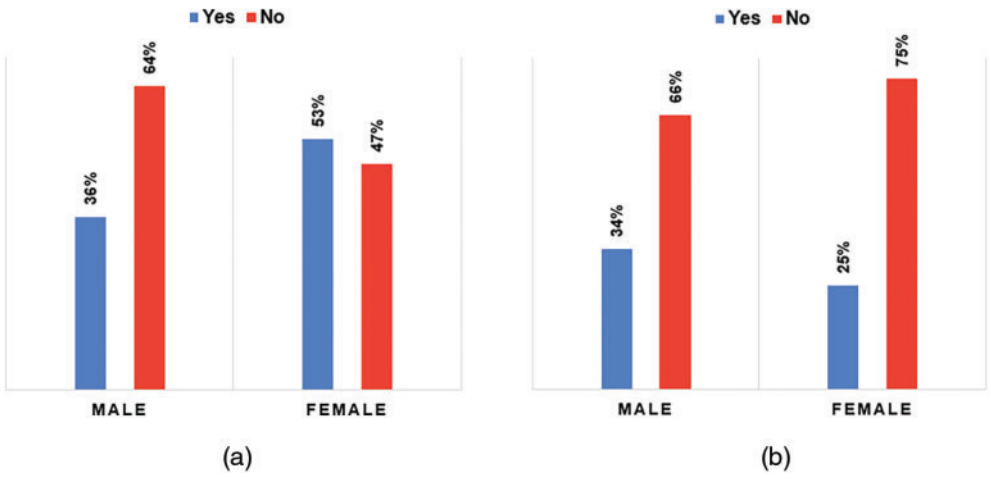

Fig. 13. Users of the (a) iOS and (b) Android system and continue using their devices in the event of changing the system.

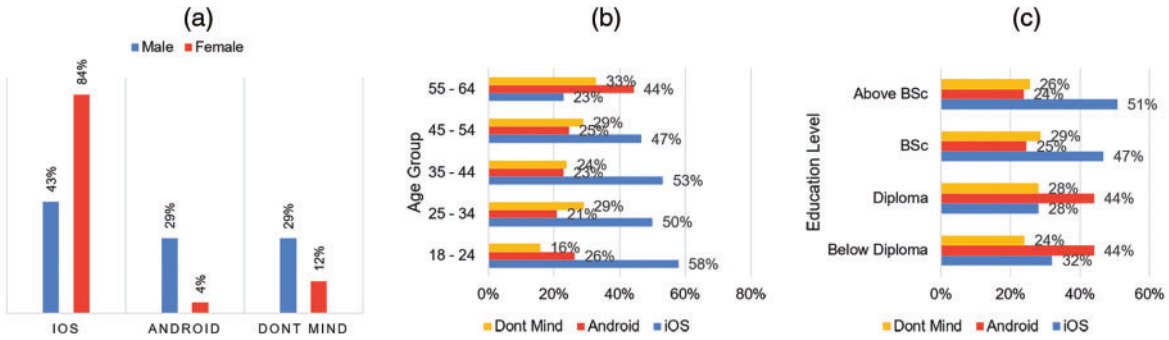

Fig. 14. The extent of participants' desire to appear in society using Android or iOS devices by: (a) gender, (b) age group, and (c) education level.

between iOS or Android system, as well as the type of device that carries these systems. In addition, it can be alleged that the desire to appear with an iOS device in social gatherings is predominant among females in most age groups and among those who have a bachelor's degree or higher.

7. Conclusion and Limitations

In conclusion, this comprehensive investigation delved into user perceptions of iOS and Android operating systems amongst a sample of 594 participants. The study, comprised of 330 iOS users and 264 Android users, revealed a nuanced interplay between factors influencing user preference, including system usability, security perceptions, social influence, and prior experiences.

While both user groups expressed confidence and trust in the reliability of their chosen system, a slight preference emerged. iOS users reported experiencing a more user-friendly interface and a heightened sense of information security on their devices. Interestingly, a potential disparity emerged between experience and perception regarding security. Android users, particularly females within this study, exhibited higher confidence in information security despite encountering a greater number of cyberattacks.

Furthermore, the study shed light on user experiences with the opposing system. A significant portion of iOS users reported positive experiences with Android, indicating a level of comfort with switching or having utilized both platforms in the past. Conversely, a quarter of Android users lacked any prior experience with iOS, potentially limiting their ability to make an informed choice. Additionally, among Android users with prior iOS experience, particularly females, the experiences were reported as neutral or even negative.

The influence of social factors on system choice emerged as another key takeaway. Age, education level, and gender all played a significant role in user decisions. The desire to be seen using an iOS device was more prevalent among females, younger users, and those with higher education. This highlights the potential impact of social perception on technology adoption, suggesting a need for both platforms to cater to the diverse motivations and preferences of users.

In conclusion, this multifaceted investigation yielded valuable insights into user perceptions of iOS and Android operating systems amongst a sample of 594 participants in Saudi Arabia. While the research design offers a robust foundation for understanding user preferences within this specific context, several limitations necessitate further exploration.

Firstly, the generalizability of the findings may be constrained by the sample size. While statistically significant within the study's parameters, a larger participant pool encompassing a broader geographical range could provide a more nuanced understanding of user preferences across diverse cultural and demographic contexts. Future research designs should prioritize the recruitment of a more internationally representative sample.

Secondly, the study's focus on participants within Saudi Arabia limits the applicability of the findings to a specific geographical and cultural context. User experiences and priorities regarding mobile operating systems may differ significantly in other regions. To create a more generalizable picture, further research efforts should be undertaken across a wider range of populations, incorporating participants from diverse geographical locations.

Thirdly, a potential gender disparity in user experience with opposing systems emerged within the findings. However, the study did not delve into the specific reasons behind this disparity, particularly among females who reported negative experiences with iOS. Investigating the underlying factors influencing these gendered differences in user experience would provide valuable insights. Future research designs should prioritize exploring these potential gender-based variations in user experience.

Despite these limitations, the study's exploration of the interplay between usability, reliability, security perceptions, social influence, and prior experiences offers a valuable foundation. By acknowledging these limitations and pursuing further research across a more diverse sample population, developers can create more user-centric experiences that cater to the multifaceted needs and preferences of a global mobile user base.

Acknowledgment

I would like to express my sincere gratitude to Umm Al Qura University for providing me with the invaluable opportunity to conduct research on software quality assurance within the field of software engineering. I would also like to extend my heartfelt thanks to my family and friends for their unwavering support and encouragement throughout this journey.

Appendix

TABLE II: iOS and Android Users

#	Question	Type of response
1.	Gender	Male
		Female
2.	Age	18–24
		25–34
		35–44
		45–54
		55–64
		65 or over
3.	What is your education level?	Below diploma
		Diploma
		BSc.
		Above BSc.
4.	What device do you prefer to be seen with in social events?	iOS device (i.e. iPhone)
		Android device (i.e. Samsung, Huawei, Honor, vivo)
		Do not mind
5.	What device do you have currently?	iOS device (i.e. iPhone)
		Android device (i.e. Samsung, Huawei, Honor, vivo)

TABLE III: iOS Users

#	Question	Type of response
1.	If you have had Android before, Rate your experience with Android	0-Very unsatisfactory 1-Unsatisfactory 2-Neutral 3-Satisfactory 4-Very satisfactory 5-Not applicable
2.	If same device you have now is using Android operating system, would you still like it?	Yes No
3.	Do you feel your information is secure with the iOS (iPhone) operating system?	0-Strongly disagree 1-Disagree 2-Neutral 3-Agree 4-Stronglly agree
4.	If you have ever encountered security issues incident with your phone, was the recovery fast and easy?	0-Strongly disagree 1-Disagree 2-Neutral 3-Agree 4-Stronglly agree 5-Not applicable
5.	Do you feel you're your Phone is reliable with the iOS (iPhone) operating system?	0-Strongly disagree 1-Disagree 2-Neutral 3-Agree 4-Stronglly agree

TABLE IV: Android Users

#	Question	Type of response
1.	If you have had iOS (iPhone) before, Rate your experience with iOS (iPhone)	0-Very unsatisfactory 1-Unsatisfactory 2-Neutral 3-Satisfactory 4-Very satisfactory 5-Not applicable
2.	If same device you have now is using iOS operating system, would you still like it?	Yes No
3.	Do you feel your information is secure with the Android operating system?	0-Strongly disagree 1-Disagree 2-Neutral 3-Agree 4-Stronglly agree
4.	If you have ever encountered security issues incident with your phone, was the recovery fast and easy?	0- Strongly disagree 1-Disagree 2-Neutral 3-Agree 4-Stronglly agree 5-Not applicable
5.	Do you feel you're your phone is reliable with the Android operating system?	0-Strongly disagree 1-Disagree 2-Neutral 3-Agree 4-Strongly agree

Conflict of Interest

The authors declare that they do not have any conflict of interest.

References

[1] I. ISO. IEC 14598-1: software product evaluation-part 1: general overview. *International Organization for Standardization*, Geneva, Switzerland. 1999.

[2] Lyu MR. *Handbook of Software Reliability Engineering*, vol. 222. IEEE Computer Society Press Los Alamitos, 1996. Accessed: Jun. 15, 2024. [Online]. Available from: https://www.academia.edu/download/28169895/56257_handbook_of_software_reliability_engineering_00_content_and_preface.pdf.

[3] Littlewood B, Strigini L. Software reliability and dependability: a roadmap. *Proceedings of the Conference on the Future of Software Engineering*, pp. 175–88, Limerick Ireland: ACM, May 2000. doi: 10.1145/336512.336551.

[4] ISO.org. *ISO/IEC 25040:2011*. 1st ed. 2011. Available from: https://www.iso.org/standard/35765.html.

[5] International Organization for Standardization. I. ISO, I. FDIS. *25020. Software Engineering—Software Product Quality Requirements and Evaluation (SQuaRE)—Measurement Reference Model and Guide*. Geneva, Switzerland: ISO; 2007.

[6] Brooke J. SUS—A quick and dirty usability scale. *Usability Eval Ind*. 1996;189(194):4–7.

[7] Bangor A, Kortum P, Miller J. Determining what individual SUS scores mean: adding an adjective rating scale. *J Usability Stud*. 2009;4(3):114–23.

[8] Reichheld FF, Markey R. *The Ultimate Question 2.0: How Net Promoter Companies Thrive in a Customer-Driven World*. Harvard business press, 2011.

[9] Reichheld FF, Covey SR. *The Ultimate Question: Driving Good Profits and True Growth*, vol. 211. Boston, MA: Harvard Business School Press, 2006.

[10] Reichheld FF. The one number you need to grow. *Harv Bus Rev*. 2003;81(12):46–55.

[11] iOS 18. Apple Developer, 2024. Accessed: Jun. 16, 2024. [Online]. Available from: https://developer.apple.com/ios/.

[12] Rana A. An overview of android operating system. *Acad Int Multidiscip Res J*. 2021;11(10):668–74.

[13] Jaiswal M. Android the mobile operating system and architecture. *Int J Creat Res Thoughts (IJCRT)*. 2018;6(1):514–25.

[14] Alliance OH. Android (operating system). *Marketing*. 2013;4(5):1–20. Accessed: Jun. 16, 2024. [Online]. Available from: https://immagic.com/eLibrary/ARCHIVES/GENERAL/WIKIPEDI/W110410O.pdf.

[15] Contributor License Agreements and Headers. Android open source project. 2024. Accessed: Jun. 16, 2024. [Online]. Available from: https://source.android.com/docs/setup/contribute/licenses.

[16] android.com. Contribute to Android | Android open source project. 2024. [Online]. Available from: https://source.android.com/docs/setup/contribute.

[17] Haris M, Jadoon B, Yousaf M, Khan FH. Evolution of android operating system: a review. *Asia Pac J Contemp Educ Commun Technol*. 2018;4(1):178–88.

[18] Van Vliet H. *Software Engineering: Principles and Practice*. 3rd ed. John Wiley and Sons, Ltd., 2008.

[19] Sommerville I. *Software Engineering*. 10th ed. Boston: Pearson, 2015.

[20] I. E. Commission. *Software Engineering-Product Quality*, vol. 9126. ISO/IEC, 2001.

[21] Miguel JP, Mauricio D, Rodriguez G. A review of software quality models for the evaluation of software products. *Int J Softw Eng Appl*. Nov. 2014;5(6):31–53. doi: 10.5121/ijsea.2014.5603.

[22] Bassler T. Experiences in introducing software quality assurance. *Annu Rev Autom Program*. 1992;16:91–4. doi: 10.1016/0066-4138(92)90014-G.

[23] Laaraib E, Maher ZA, Solangi ZA, Koondhar MY, Mukhtiar MM, Shah A. A methodology for incorporating quality assurance practices during software development life cycle. *Int J*. 2021;10:2296–301.

[24] Xenos M. Usability perspective in software quality. *Usability Engineering Workshop, The 8th Panhellenic Conference on Informatics with International Participation*. Southern Cyprus, 2001. Accessed: Jun. 15, 2024. [Online]. Available from: https://www.researchgate.net/profile/Michalis-Xenos/publication/228983955_Usability_perspective_in_software_quality/links/00b7d527a68a01c920000000/Usability-perspective-in-software-quality.pdf.

[25] Febrero F, Calero C, Moraga MÁ. Software reliability modeling based on ISO/IEC SQuaRE. *Inf Softw Technol*. 2016;70:18–29.

[26] ISO. ISO/IEC 25010:2023(En). 2023.

[27] Nance KL, Strohmaier M. End user perception and software quality assessment. *J Int Inf Manag*. 1997;6(1):1.

[28] Green GC, Hevner AR, Collins RW. The impacts of quality and productivity perceptions on the use of software process improvement innovations. *Inf Softw Technol*. 2005;47(8):543–53.

[29] Gefen D, Straub DW. Gender differences in the perception and use of e-mail: an extension to the technology acceptance model. *MIS Quarterly*. 1997;21(4):389–400.

[30] Mohammadi H. Investigating users' perspectives on e-learning: an integration of TAM and IS success model. *Comput Hum Behav*. 2015;45:359–74.

[31] Oh T, Stackpole B, Cummins E, Gonzalez C, Ramachandran R, Lim S. Best security practices for android, blackberry, and iOS. *2012 The First IEEE Workshop on Enabling Technologies for Smartphone and Internet of Things (ETSIoT)*, pp. 42–7. IEEE, 2012. Accessed: Jun. 16, 2024. [Online]. Available from: https://ieeexplore.ieee.org/abstract/document/6311252/.

[32] Ahmad MS, Musa NE, Nadarajah R, Hassan R, Othman NE. Comparison between android and iOS operating system in terms of security. *2013 8th International Conference on Information Technology in Asia (CITA)*, pp. 1–4. IEEE, 2013. Accessed: Jun. 16, 2024. [Online]. Available from: https://ieeexplore.ieee.org/abstract/document/6637558/.

[33] Pieterse H, Olivier M, Van Heerden R. "Detecting manipulated smartphone data on android and iOS devices," in *Information Security*, vol. 973. In *Communications in Computer and Information Science*. vol. 973,Venter H, Loock M, Coetzee M, Eloff M, Eloff J, Eds. Cham: Springer International Publishing, 2019, pp. 89–103, doi: 10.1007/978-3-030-11407-7_7.

[34] Götz FM, Stieger S, Reips U-D. Users of the main smartphone operating systems (iOS, Android) differ only little in personality. *PloS One*. 2017;12(5):e0176921.

[35] Adekotujo A, Odumabo A, Adedokun A, Aiyeniko O. A comparative study of operating systems: case of windows, unix, linux, mac, android and ios. *Int J Comput Appl*. 2020;176(39):16–23.

[36] Hu W, Hao T, Hu Y, Chen H, Zhou Y, Yin W. Research on the brand image of iOS and Android smart phone operating systems based on mixed methods. *Front Psychol*. 2023;14:1040180.

[37] Al-Qershi F, Al-Qurishi M, Rahman SMM, Al-Amri A. Android vs. iOS: the security battle. *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, pp. 1–8. IEEE, 2014. Accessed: Jun. 16, 2024. [Online]. Available from: https://ieeexplore.ieee.org/abstract/document/6916629/.

[38] Wukkadada B, Nambiar R, Nair A. Mobile operating system: analysis and comparison of Android and iOS. *Int J Comput Technol*. 2015;2(7):273–6.

[39] Mohamed I, Patel D. Android vs iOS security: a comparative study. *2015 12th International Conference on Information Technology-New Generations*, pp. 725–30. IEEE, 2015. Accessed: Jun. 16, 2024. [Online]. Available from: https://ieeexplore.ieee.org/abstract/document/7113562/.

[40] Garg S, Baliyan N. Comparative analysis of Android and iOS from security viewpoint. *Comput Sci Rev*. 2021;40:100372.

[41] Sahani A. Android v/s IOS—The unceasing battle. *Int J Comput Appl*. 2017;180(3):23–6.

[42] Gyorodi R, Zmaranda D, Adrian VG, Gyorodi C. A comparative study between applications developed for android and ios. *Int J Adv Comp Sci Appli*. 2017;8(11):176–82.

[43] Susanto H, Almunawar MN, Leu F-Y, Chen CK. Android vs iOS or others? SMD-OS security issues: generation y perception. *Int J Technol Diffus IJTD*. 2016;7(2):1–18.

[44] Bhardwaj A, Pandey K, Chopra R. Android and ios security-an analysis and comparison report. *Int J Inf Securi Cyber*. 2016;5(1):32–44.

[45] Lazareska L, Jakimoski K. Analysis of the advantages and disadvantages of Android and iOS systems and converting applications from Android to iOS platform and vice versa. *Am J Softw Eng Appl*. 2017;6(5):116–20.

[46] Zeydan E. Android vs. IOS: a comparative analysis over mobile operator infrastructures based on crowdsourced mobile dataset. *Telecommun Syst*. Nov. 2021;78(3):405–19. doi: 10.1007/s11235-021-00820-y.

[47] Hayran A, İğdeli M, Yılmaz A, Gemci C. Security evaluation of IOS and Android. *Int J Appl Math Electron Comput*. 2016;(Special Issue–1 (December)):258–61.