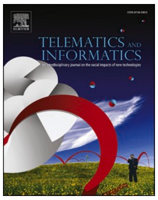
Telematics and Informatics 58 (2021) 101535

Contents lists available at ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele



# Understanding the asymmetric perceptions of smartphone security from security feature perspective: A comparative study

Quan Xiao

*School of Information Management, Jiangxi University of Finance and Economics, Nanchang 330032, China*

ARTICLE INFO

*Keywords:*
Smartphone security
Security feature
Developer and user
Android vs iOS
Gender difference
Kano model

ABSTRACT

Smartphones are being used and relied on by people more than ever before. The open connectivity brings with it great convenience and leads to a variety of risks that cannot be overlooked. Smartphone vendors, security policy designers, and security application providers have put a variety of practical efforts to secure smartphones, and researchers have conducted extensive research on threat sources, security techniques, and user security behaviors. Regrettably, smartphone users do not pay enough attention to mobile security, making many efforts futile. This study identifies this gap between technology affordance and user requirements, and attempts to investigate the asymmetric perceptions toward security features between developers and users, between users and users, as well as between different security features. These asymmetric perceptions include perceptions of quality, perceptions of importance, and perceptions of satisfaction. After scoping the range of smartphone security features, this study conducts an improved Kano-based method and exhaustively analyzes the 245 collected samples using correspondence analysis and importance satisfaction analysis. The 14 security features of the smartphone are divided into four Kano quality types and the perceived quality differences between developers and users are compared. Correspondence analysis is utilized to capture the relationship between the perceived importance of security features across different groups of respondents, and results of importance-satisfaction analysis provide the basis for the developmental path and resource reallocation strategy of security features. This article offers new insights for researchers as well as practitioners of smartphone security.

## 1. Introduction

As one of the most pervasive information and communication technologies, the world has witnessed a dramatic development of smartphones in the last decade (Lopez-Fernandez et al., 2017; Verkijika, 2018). A smartphone is an intelligent device with an intuitive user interface and operating system that can access the Internet and provide users with a large number of functional features by installing various applications (Wang et al., 2014). Smartphones expand the positive user experience by keeping people connected, engaging in new forms of gaming and media entertainment, or achieving comfort with health tracking apps (Kraus et al., 2017; Liu et al., 2020a). As CNNIC(2020) reported, by March 2020 the size of China’s mobile Internet users reached 897 million, with 99.3% of Internet users using mobile phones to access the Internet, the vast majority of whom are smartphone users. Similar cases are seen in the United States and other Asian countries such as South Korea and Singapore (Kim et al., 2015; Gartner, 2020; Newzoo, 2019), as well as less developed areas due to the far less ownership cost of smartphones than computers (Bonnington, 2015). Google recently announced

*E-mail address:* xiaoquan@foxmail.com.

https://doi.org/10.1016/j.tele.2020.101535
Received 8 May 2020; Received in revised form 9 September 2020; Accepted 12 November 2020
Available online 18 November 2020

that its active Android devices surpassed 2.5 billion (Brandom, 2019).

Although people benefit from the functionalities and conveniences of smartphones, the open interconnectivity of smartphones exposes more and more of themselves to malware authors (Qamar et al., 2019; Alazab, 2014). Smartphone users are facing numerous security and privacy threats such as malicious apps, financial losses, data breaches, network surveillance, and so on (Jones and Chin, 2015; Kraus et al., 2017). A recent report from Kaspersky Lab revealed that in 2019, Kaspersky mobile products and techniques detected 3,503,952 malicious installation packages, 69,777 new mobile banking Trojans, and 68,362 new mobile ransomware Trojans, and the number of attacks on the personal data of mobile device users increased by half: from 40,386 unique users in 2018 to 67,500 in 2019. (Chebyshev, 2020). These security threats severely impact the confidentiality, integrity and availability of mobile data and systems (Farivar et al., 2020), especially in the current situation where many people seem unable to live without leaving their smartphones (Hertlein, 2012; Verkijika, 2018).

As smartphone users, we are exposed to security risks at all stages during our daily use of our smartphones (Alavi and Buttlar, 2019). When downloading a mobile app, the app may have been implanted with malicious code. Faruki et al. (2015) noted that most Android malware is repackaged into other legitimate popular apps to bypass security detections. Although iOS is usually considered more secure than Android due to its strict app review mechanism, some studies have shown that some iOS app developers can code through tampered unofficial Xcode development tools (Yao et al., 2018). When an app is installed or first opened, it is usually asked to grant it some permissions such as GPS location, camera and microphone enabling, address book access, etc. Developers tend to ask for more permissions than they actually need, and it is difficult for users to assess what the consequent risks are after granting those permissions (Jorgensen et al., 2015). When we click on a link sent by a friend, we may be hit by a Trojan horse, and when scanning a QR code, we may enter a phishing site. Not only do malicious programs send and receive malicious messages, sabotage systems, snoop on privacy, and steal accounts without the user's notice while using the smartphone, but they keep updating themselves with new features to improve viability (Alazab et al., 2020). Even in the face of being uninstalled, some apps cannot be thoroughly cleaned up, leaving some malicious residual code behind. Therefore, the security of smartphone is a critically important topic that requires both academia and industry to figure out its implications and seek protection against various mobile security threats (Wang and Lee, 2020).

In addition to the security-related features that come with smartphones, there are many mobile security apps available in Google Play and Apple app stores, where we get a sense of the efforts of the developers on smartphone security, but users are far less enthusiastic about these mobile security apps (in terms of downloads and usage) than how they behave on PCs. Many of them place an emphasis on the appearance and performance aspects of the smartphone over security issues, or just try to use a small fraction of the many security designs available. Yao et al. (2018) argue that users may be confused by the unnecessary security features, which lead to the distractions, operating clumsiness and interferences and suggest that the concerns of females and low technology familiarity users on security features differ from that of males and users with high technology familiarity. From the above analysis, it can be noticed that in the face of such a harsh smartphone security environment, on the one hand, smartphone security designers and developers have made unremitting efforts, while on the other hand, these efforts have been met with indifference from users. Past research paradigms that looked at smartphone security as a holistic whole to examine user needs and adoption from a macro perspective, have struggled to capture the mechanisms behind this gap, making micro-studies from the perspective of design features a possible solution. At this point, it is plausible to speculate that there may be different understandings between users and developers, and also differences in the extent to which different security features are used and valued. These objectively existing but unidentified differences are not conducive to effective design by smartphone security policy designers to meet the differentiated needs of users. Such asymmetric understandings result in a gap between the significance of smartphone security and the lack of actual adoptions, which motivates this study to address the following three research questions.

RQ1: What asymmetrical needs do smartphone users have for different security features?

RQ2: Is there an asymmetry in the appraisal for security features between developers and users, and between different types of users?

RQ3: What route should smartphone security strategy designer follow to foster user satisfaction on smartphone securities?

In efforts to seek answers to the questions, this study first introduces the Kano model to classify smartphone security features to capture users' nonlinear needs toward different security features. Next, a Kano analysis and correspondence analysis is conducted on the sample data from different groups to grasp the differences in security feature requirements between developers and users, and between users with different characteristics (i.e., male versus female, iOS versus Android). Finally, importance-satisfaction analysis is used to obtain the best path for smartphone security policy design.

The remainder of the paper is organized as follows. In Section 2 related works in terms of smartphone security and Kano model are reviewed. Section 3 presents the research methodology, which detailedly demonstrates the process for security feature selection, Kano quality classification, correspondence analysis and IPA. The results are shown and discussed in Section 4. Section 5 presents the implications, limitations and conclusions.

## 2. Related works

### 2.1. Smartphone security

Computer and Internet security has been well studied over the past few decades (Siponen, 2002), and the smartphone boom in recent years has led scholars to focus on the security of smartphones. Compared to personal computers, smartphones are more vulnerable (Choi and Lee, 2012) because they are now a must-have item for everyone and a large number of tasks involving personal privacy are performed through them, such as sending and receiving emails, socializing, shopping and transferring money (Yao et al., 2018; Zhang et al., 2018). Existing research on smartphone securities is conducted in three main streams. The first research stream focused on the source of the smartphone threat. Common sources of cyber-attacks include virus, phishing attack, Trojan horse, worm, ransomware, spyware, unauthorized access, control system attacks and so on (Srinivas et al., 2019). Through a survey on security for mobile devices, La Polla et al. (2013) categorized the methods of attack on mobile devices as wireless, break-in, infrastructure-based, worm-based, botnet, and user-based, while summarized the goals of the attacks as privacy, sniffing, denial of service and overbilling. Zaidi et al.(2016) further classify attacks on smartphones into old and new attacks, where old attacks include physical attacks, radio and wireless network attacks, backdoor, virus, worms, malware, Trojan, spam and threat, while new attacks include relay attacks, cold boot attack, brute force attack, denial of service attack, smudge attack, cross-site scripting (XSS) attack, etc.

The second research stream explores smartphone security technologies and security solutions from the designer's perspective. For example, in terms of the permission management, several solutions including improved information presentation and risk communication were proposed to improve user's understanding and attention to permissions, (Harbach et al., 2014; Kraus et al., 2014). Earlier versions of Android required users to accept full permissions when installing an app, whereas after version 6.0 it allowed individual permission settings for each app (Oldenburg, 2015). In order to protect authorized access to mobile phones, biometric-based authentication technologies such as Touch ID, fingerprint recognition, face recognition, etc. have emerged on top of past PIN codes and passwords (Bhagavatula et al., 2015). Similar to personal computers, anti-virus and anti-malware applications can also be installed in smartphones for security (Fan et al., 2014). In addition, some scholars have proposed a number of smartphone security technologies and solutions for specific security threats (Hussain et al., 2018). Enck et al. (2010) designed an information-flow tracking system called TaintDroid to monitor whether important data stored on a smartphone is being transmitted by untrusted apps and can notify users in real time. Dini et al. (2018) proposes a MAETROID framework that evaluates the trustworthiness of an app to be installed by combining information such as the app's permission requirements and the quality and popularity of the app provided by the app store to determine whether it is safe or dangerous. Mishra and Soni (2020) designed a model named "Smishing Detector" to detect and block smishing attacks through SMS content analysis and URL behavior analysis. Zulkefli and Singh (2020) proposed a smartphone access control model named SENSATE by integrating role- and attribute-based and multilevel security to fight against smartphone cybercrimes such as advanced persistent threat.

Exploring smartphone security in terms of user attitudes and behaviors from user's perspective is the third research stream to be concerned with. In a survey by Felt et al. (2012), they asked 3115 smartphone users to rate their concern about the 99 risks of smartphone permissions, where the top three risks were permanently disable your phone, made phone calls to 1–900 numbers and sent premium text messages from your phone. Another study on user attitudes towards smartphone security and privacy, completed by Chin et al. (2012), showed that the reasons why users are worried about performing privacy-sensitive and financially sensitive tasks on their phones include physical theft or damage, data loss, mistrust of smartphone applications, wireless network attacks, accidental touch or click, and so on. Currently, user awareness of smartphone security is weak and user acceptance of the various authorization methods offered is low (Breitinger and Nickel, 2010). Imgraben et al. (2014), for example, point out that many users are unaware of the risks they may suffer by leaving Wi-Fi and Bluetooth on all the time, and argue that educational training and awareness programs are crucial to rectify misperceptions and usage behavior. In a recent investigation on the contending attitude of commuters towards the geolocation data collection of smartphone, Cabalquinto and Hutchins (2020) grouped the attitudes into six categories as in favour, in favour with guarantees, sceptical, staunchly opposed, confused and apathetic, and suggested the publicly visible initiatives to raise the awareness are essential. Kraus et al. (2017) conducted an online survey to quantify psychological need fulfillment for security and privacy actions on smartphones and found keeping the meaningful, stimulation, autonomy and competence to be salient motivators for security and privacy actions on smartphones. Verkijika modified the PMT by including anticipated regret as mediator to test the relationship between threat dimensions of the PMT and security intentions and behaviors. Through a survey to understand smartphone user's choices, awareness and education toward cybersecurity, Breitinger et al. (2020) indicated that smartphones are less secure than desktop computers, and fewer third-party security products are installed.

While the importance of smartphone security is prompted by a range of risk and loss data from the industry, there is much evidence that users do not value smartphone security. For example, Mylonas et al. (2013) found that 76% of users believe that apps downloaded from the app repository are safe, they tend to turn off smartphone security features and prefer to use pirated apps, while Alani (2017) indicated that only 35% of users would review the permissions required for the app. In a case study of update installation behavior, Moller et al. (2012) found that many users do not install updates in time to enhance the security of their smartphones, while Ameen et al. (2020) compared smartphone security behavioural intention among employees in the United Arab Emirates and the United States, and found that employees in both countries are insufficiently aware of the risks arising from smartphone use. Technical researchers and security developers have made various efforts to detect, judge, and block malware and attacks, and have developed mobile security apps to keep smartphones safe, but users are not buying it, and many question the effectiveness of security software (Fedler et al., 2013), and believe that installing the security app is unnecessary (Mylonas et al., 2013).

I address that in terms of smartphone security, despite the industry's emphasis on the seriousness of threats, there is a considerable asymmetry between what the technology and developers are pouring in and what users perceive. Although various security technologies and solutions have been proposed, there is a lack of systematic overviews toward the security features offered by smartphones. Most existing researches examining smartphone user security behaviors holistically, providing solutions, or targeting specific security features are not conducive to the clarity of this research area, and may create confusion for users when faced with such a complex array of the security features. Currently, inter-user differences in smartphone security features and behaviors have garnered the attention of several studies, Yao (2018), for example, noted that women are more concerned than men about the "remote locate and lock" and "Wi-Fi security", while users at different levels of technology familiarity have different concerns about security features. Ameen (2020) further investigated the differences of employee's behavioral intention to smartphone in a cross-national context.

However, many of the current findings are still preliminary and trivial, and in-depth exploration of asymmetric perception of smartphone security features is still far from adequate. From a microscopic feature-based perspective, systematically sorting out the current smartphone security features provided and capturing the various potential asymmetries therein constitutes the crux of the study's concern: to understand the asymmetry perceptions between smartphone developers and users, as well as users with different characteristics, toward the various security features for smartphones, and provide pathfinders for smartphone security policy designers on how to rationally provide security features.

## 2.2. *Kano model*

Smartphones offer a wide variety of security features, but the reality is that users do not treat these security features equally, and their needs and satisfaction with different security features are non-linear and asymmetric. When it comes to portraying asymmetries in users' perceptions of the quality attributes of a product or service, the Kano model is a very representative approach (Ting and Chen, 2002). It is traditionally accepted that user satisfaction is positively proportional to performance level (Liu et al., 2020b), i.e., the higher the performance level, the higher the satisfaction level and vice versa, which is knows as one-dimensional quality theory (Chen and Chuang, 2008). Stemming from Herzberg's two-factor theory, the Kano model, a two-dimensional quality theory was proposed in 1984 (Kano et al., 1984), which classifies product quality attributes into five categories, namely, must-be quality, one-dimensional quality, attractive quality, indifferent quality, and reverse quality, based on the relationship between the objective performance of the product quality attributes and the subjective perceptions of the users (Kopackova and Komarkova, 2020). Fig. 1 shows the Kano model's depiction of the characteristics of the five types of product quality attributes.

In the Kano model, the case in which the performance of an attribute is positively proportional to user satisfaction is called a one-dimensional quality attribute. However, if the degree of fulfillment of an attribute is disproportionate to user satisfaction, e.g. the fulfillment of this attribute (functional) does not increase user satisfaction, but its non-fulfillment (dysfunctional) causes user dissatisfaction, this attribute is called a must-be quality. Conversely, an attribute is defined as attractive if its non-fulfillment does not result in user dissatisfaction, but if its implementation once would result in user satisfaction. If an attribute has no effect on user satisfaction or dissatisfaction, whether functional or dysfunctional, then it is called an indifferent quality. Reverse quality is characterized by the fact that its fulfillment results in user dissatisfaction and that users will be satisfied when it is not fulfilled, which is rare in reality, and is seldom considered by existing studies (Chen, 2012).

To date, a number of studies based on the Kano model have emerged. Part of this focuses on methodological improvements to the Kano model, while the other part attempts to apply the Kano model to different domains in order to obtain new insights that distinguishing from previous investigations based on one-dimensional quality theory. In terms of methodological improvements, Lin et al. (2010) proposed a moderated regression approach to produce more accurate attribute classification. Lee and Huang (2009) applied an approach of fuzzy questionnaires to modify Kano's two-dimensional questionnaires. Additionally, penalty-reward contrast analysis,

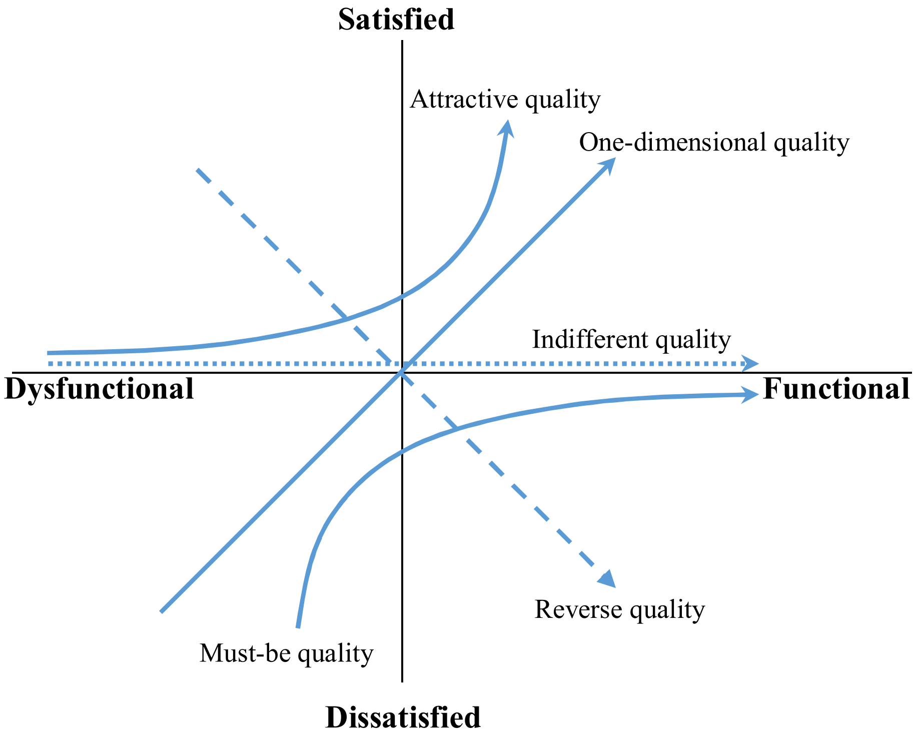


**Fig. 1.** The Kano model.

importance grid analysis, and neural network are also integrated with Kano model to classify quality attributes (Chen, 2012). There are more studies about the application of the Kano model, such as e-commerce website design (Ilbahar and Cebi, 2017), web content recommendation (Chang et al., 2009), mobile security applications (Yao, et al, 2018), sports lesson programs (Bu and Park, 2016), new product design (Tontini, 2007), logistics customer service (Florez-Lopez and Ramon-Jeronimo, 2012) and tourism management (Go and Kim, 2018).

In the case of smartphone security studied in this paper, although today's smartphones offer a range of security features to help users shield themselves from insecurity, users' perceptions of the quality, importance, and satisfaction toward these security features are not the same across features, and these perceptions may differ across user groups. With the exception of a very small number of studies, such as the analysis of mobile security application features by Yao et al. (2018), the asymmetric perceptions of users of these security features for smartphones are not addressed. Following the "performance-satisfaction" asymmetry of the Kano model, this paper attempts to refine the current problems of the Kano model and, in conjunction with correspondence analysis as well as importance-satisfaction analysis, to fill the research gaps in this issue.

## 3. Method

The research methodology proposed in this study consists of three stages, as shown in Fig. 2. Based on the first phase of smartphone security feature selection, a Kano-based classification is conducted in the second phase to understand the asymmetric perceptions of quality between security features as well as between respondents. The third phase consists of two pathways, using correspondence analysis and importance-satisfaction analysis, respectively, to capture the asymmetric perceptions of importance and satisfaction of security features between respondents. Thus, insights into the design of smartphone security features are obtained.

### 3.1. Security features selection

In order to proceed with the analyses proposed in this study, the construction of smartphone security feature repertoire is the first foundation to be completed. The rationale for the construction comes from three main sources. First, by collecting the existing

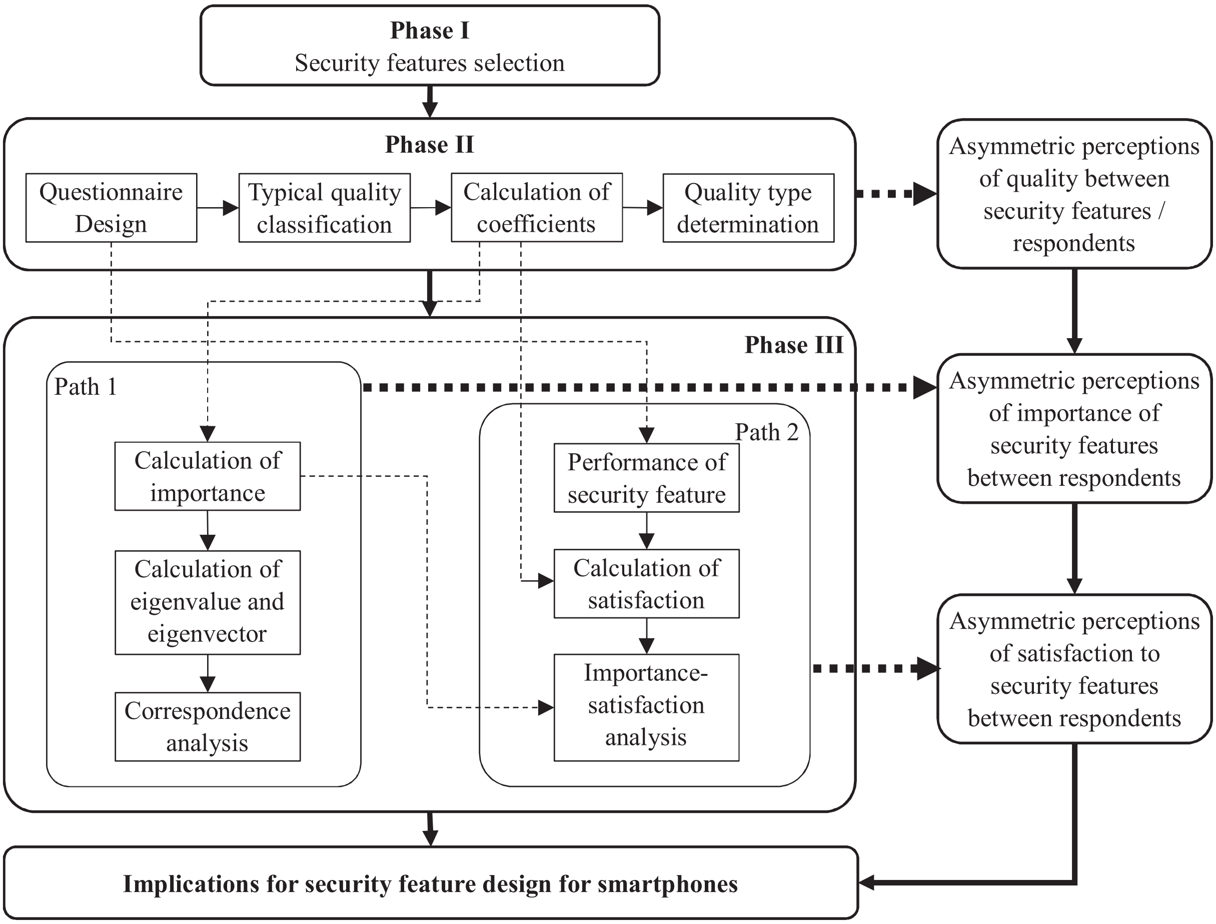

Phase I
Security features selection
Phase II
Questionnaire Design
Typical quality classification
Calculation of coefficients
Quality type determination
Asymmetric perceptions of quality between security features / respondents
Phase III
Path 1
Calculation of importance
Calculation of eigenvalue and eigenvector
Correspondence analysis
Path 2
Performance of security feature
Calculation of satisfaction
Importance-satisfaction analysis
Asymmetric perceptions of importance of security features between respondents
Asymmetric perceptions of satisfaction to security features between respondents
Implications for security feature design for smartphones

**Fig. 2.** Proposed research framework.

literature on smartphone security, extract the security features of each study that are of interest (e.g., from research topics, technical considerations), and summarize them. Secondly, the security features referred to by smartphone manufacturers, as well as Apple (iOS) and Google (Android) are extracted from the documentation describing the security of smartphones and related operating systems. Third, an analysis of existing smartphone security apps (e.g. AhnLab V3 Mobile Security, Antiy AVL, 360 Mobile Security, etc.) on the market to investigate their usability, security feature affordance and the protection they can provide. By integrating all the identified smartphone security features, the final repertoire of security features was obtained for this study as Table 1.

### *3.2. Kano-based classification*

This paper builds upon the Kano model to analyze the asymmetry of users' perceptions of different security features of smartphones, and how these perceptions differ between different user groups. According to the basic process of Kano model analysis, the questionnaire needs to be designed first. The traditional Kano model primarily measures user satisfaction when quality attributes are fulfilled or not through a set of two-way questionnaires. In addition to grasping users' perceptions of the quality of smartphone's security features, this study is also dedicated to capture users' perceptions in terms of importance, performance and satisfaction, which leads to subsequent correspondence analysis, importance-satisfaction analysis, and comparisons between groups. To this end, the questionnaire was designed as shown in Table 2, which also demonstrates the logic among the analyses to be conducted in the study.

In terms of the perceptions of quality, respondents' answers to the two-way questionnaire made up a total of 25 (5*5) possible combinations. The Kano model designed a typical quality classification table for these possible scenarios, as shown in Table 3. For example, if a user chooses "Like" when the security feature "App Permission Management" is fulfilled, but is "Dislike" when not fulfilled, then the typical quality type of "App Permission Management" for that user is "One-dimensional".

After all respondents have completed the two-way questionnaire and their respective typical quality types for all security features are identified, the scrutiny of the frequency distribution of each security feature is the most common Kano quality classification method. The type of quality with the highest frequency reflects the respondent's dominant judgment (Lofgren and Witell, 2008). However, this convenient calculation has been criticized as being too simple and lacking in representativeness if a quality type cannot achieve half agreement (Lee and Huang, 2009). And, when the highest frequency of multiple quality types are similar, it is inappropriate to ignore the followed types entirely. Many studies based on the traditional Kano model get mostly indifferent quality and one-dimensional quality (Bu and Park, 2016; Yao et al., 2018). Followed by Berger (1993), this study determines the quality type of a security feature by calculating its satisfaction coefficient and dissatisfaction coefficient, and comparing the relationship between these two coefficients and their average for all security features.

For security feature $sf_j$, the satisfaction coefficient is calculated as: $SC_j = \frac{A_j+O_j}{A_j+O_j+M_j+I_j}$, where $A_j$, $O_j$, $M_j$ and $I_j$ represents the frequency of security feature $sf_j$ on attractive quality, one-dimensional quality, must-be quality and indifferent quality within the traditional Kano model respectively. The higher satisfaction coefficient of security feature $sf_j$, the stronger the positive impact of performance improvement of $sf_j$ on satisfaction. In turn, the dissatisfaction coefficient of security feature $sf_j$ is calculated as: $DSC_j = \frac{O_j+M_j}{A_j+O_j+M_j+I_j}$, where the symbolic meanings are the same as satisfaction coefficient. A higher value of the dissatisfaction coefficient for a security

**Table 1**
Smartphone security feature repertoire for the study.

| No | Security feature (Abbr.) | Description |
|---|---|---|
| 1 | Banking and Payment Security (BPS) | To ensure the security of bank accounts and the payment process. |
| 2 | Fraud and Harassment Prevention (FHP) | Automatic blocking or flagging of unknown calls or messages to prevent fraud or harassment. |
| 3 | Malware Prevention (MP) | To prevent malicious software from being downloaded and installed through strict censorship and filtering. |
| 4 | Scanning Virus and Trojans (SVT) | Detect viruses and Trojans in apps and files on smartphone whenever. |
| 5 | App Encryption and Lock (AEL) | Encryption or locking of designated apps to ensure authorized app access and data privacy. |
| 6 | App Permission Management (APM) | Setting of permissions for the apps to obtain location, read contacts, make phone calls, send text messages, start the camera, background network access, etc. |
| 7 | Mobile Phone Anti-theft (MPA) | View the smartphone's latest location information in the event it is lost, or remotely wipe the data or lock the smartphone to help locate it or prevent illegal use. |
| 8 | Network and Traffic Management (NTM) | Manage network access of applications, to view and control traffic usage. |
| 9 | Wi-Fi Security (WS) | Provides encryption and protection against data interception, information theft, and Trojans implantation when connecting to a public or unknown Wi-Fi network. |
| 10 | Battery Management (BM) | Keeping abreast of battery usage and turning off unnecessary features to save power. |
| 11 | Data Backup (DB) | Back up the apps and the within data to external storage devices or cloud spaces |
| 12 | Cache and Garbage Cleanup (CGC) | Scan and clean up cached files and garbage files that are generated during the use of the smartphone. |
| 13 | URL and QR Code Security (UQCS) | Prevents access to malicious pages or phishing sites when users click on URL links or scan QR codes. |
| 14 | System Restoration and Rescue (SRR) | In the event of a system failure, recover the files in the smartphone or even the entire operating system to prevent the loss of important data. |

**Table 2**
The questionnaire design.

| Aspects | Questions and measurements | Objectives |
|---|---|---|
| Perceptions of quality | What is your level of satisfaction when the "data backup" security feature is (not) fulfilled by a smartphone? [dislike, live-with, neutral, must-be, like] | To understand respondents' requirement modes for different security features and use them for quality classification of security features. |
| Perceptions of importance | Not measured directly. [It is derived from Kano two-way items in this study] | To capture respondents' preferences for the importance of different security features of smartphone for the follow-up correspondence analysis and importance- satisfaction analysis. |
| Perceptions of performance | How would you rate the performance of the "data backup" security feature? [From 1 to 10] | To obtain the respondents' evaluation of the performance of security features of smartphone for the calculation of the satisfaction. |
| Perceptions of satisfaction | Not measured directly. [Calculated based on perceptions of quality and performance] | To capture respondents' satisfaction toward security features of smartphone for the conduct of importance-satisfaction analysis. |
| Sample groups | Demographic characteristics, mobile phone operating systems, whether or not engage in IT development-related work. | To understand how respondents' perceptions of the quality, importance, and performance of smartphone security features differ across demographic characteristics (e.g., male and female), operating systems (e.g., iOS and Android), and between users and developers. |

**Table 3**
Typical quality classification table.

| Functional | Dysfunctional | | | | |
|---|---|---|---|---|---|
| | Like | Must-be | Neutral | Live-with | Dislike |
| Like | Q | A | A | A | O |
| Must-be | R | I | I | I | M |
| Neutral | R | I | I | I | M |
| Live-with | R | I | I | I | M |
| Dislike | R | R | R | R | Q |

Notes: M (must-be quality), O (one-dimensional quality), A (attractive quality), I (indifferent quality), R (reverse quality), Q (questionable quality). Sourced by Matzler and Hunterhuber (1998).

feature indicates that its nonfulfillment will lead to greater dissatisfaction.

Next, the average of the satisfaction coefficient for all security features is calculated as $\overline{SC} = \frac{1}{\mathrm{f}}\sum_{j=1}^{f} SC_j$, while the average dissatisfaction coefficient calculated as $\overline{DSC} = \frac{1}{\mathrm{f}}\sum_{j=1}^{f} DSC_j$, where $f$ is the number of all security features. Then the quality type of security feature $sf_j$, denoted by $QT_j$, is determined by the following rules:

$$QT_j = \begin{cases} One-dimensional, & SC_j \geq \overline{SC} \& DSC_j \geq \overline{DSC} \\ Attractive, & SC_j \geq \overline{SC} \& DSC_j < \overline{DSC} \\ Indifferent, & SC_j < \overline{SC} \& DSC_j < \overline{DSC} \\ Must-be & SC_j < \overline{SC} \& DSC_j \geq \overline{DSC} \end{cases}$$

By performing the above analysis on all the collected samples, it is possible to obtain the quality classification of each security feature of smartphone at the level of all the respondents, i.e. to understand their different perceptions of the quality toward different security features. It is also possible to select a portion of the sample for analysis to capture the subsample's classification of the quality of security features, or to make intergroup comparisons.

### *3.3. Correspondence analysis*

Correspondence analysis is a multivariate statistical technique that reveals associations between variables by analyzing a cross tabulations (or cross tabs, contingency tables) composed of qualitative variables (Hoffman and Frank, 1986), which visually transform cross-tabulations of row and column variables into scatterplots, and presents the correlations between categorial variables in terms of spatial location (De Leeuw and Mair, 2009). The advantage of correspondence analysis is that when investigating multiple categorial variables, the plots are presented in a straightforward and easier-to-interpret manner, and when the qualitative variables are divided into more categories, the advantages of this approach are more obvious. Correspondence analysis has proven to be a useful approach in applications such as sociology (Gerhards and Anheier, 1989), ecology (James and McCulloch, 1990), psychology (Doey and Kurta, 2011) and marketing (Hoffman and Frank, 1986). In this study, correspondence analysis is employed to describe the associations between security features of smartphone and data samples.

Suppose $X = (x_{ij})_{n\times f}$ is the normalized data matrix where $n$ denotes the number of data samples and $f$ represents the number of security features. Calculate matrix $Z$ as follows:

$$z_{ij} = \frac{x_{ij} - P_i \bullet P_j / P}{\sqrt{P_i \bullet P_j}}$$

where $P_i = \sum_{j=1}^{f} x_{ij}$, $P_j = \sum_{i=1}^{n} x_{ij}$, $P = \sum_{i=1}^{n}\sum_{j=1}^{f} x_{ij}$.

Then calculate the eigenvalues of $A = Z'Z$ as $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r$ $(0 < r \leq \min\{f,n\})$ and normalize the corresponding eigenvectors $\mu_1, \mu_2, \cdots, \mu_r$. The dominant eigenvalues and their eigenvectors yield R-type factor loading matrix:

$$F = \begin{bmatrix} \mu_{11}\sqrt{\lambda_1} & \mu_{12}\sqrt{\lambda_2} & \cdots & \mu_{1m}\sqrt{\lambda_m} \\ \mu_{21}\sqrt{\lambda_1} & \mu_{22}\sqrt{\lambda_2} & \cdots & \mu_{2m}\sqrt{\lambda_m} \\ \cdots & \cdots & \cdots & \cdots \\ \mu_{f1}\sqrt{\lambda_1} & \mu_{f2}\sqrt{\lambda_2} & \cdots & \mu_{fm}\sqrt{\lambda_m} \end{bmatrix}$$

Similarly, calculate and normalize the eigenvectors $v_i = Z\mu_i$ of $A = ZZ'$, and the Q-type factor loading matrix is obtained:

$$G = \begin{bmatrix} v_{11}\sqrt{\lambda_1} & v_{12}\sqrt{\lambda_2} & \cdots & v_{1m}\sqrt{\lambda_m} \\ v_{21}\sqrt{\lambda_1} & v_{22}\sqrt{\lambda_2} & \cdots & v_{2m}\sqrt{\lambda_m} \\ \cdots & \cdots & \cdots & \cdots \\ v_{f1}\sqrt{\lambda_1} & v_{f2}\sqrt{\lambda_2} & \cdots & v_{fm}\sqrt{\lambda_m} \end{bmatrix}$$

Thus, the scatter plots of security features and data samples in the plane of the factor axis can be drawn. In the current study, correspondence analysis is used to capture respondents' perceptions of the importance of smartphone security features across different groups. In the questionnaire shown in Table 2, items on perceptions of importance are not included. It was not measured directly because respondents' preferences for the importance of security features are already implicit in the Kano two-way questions that measure quality perceptions. The higher the satisfaction and dissatisfaction coefficients of a security feature, the greater the impact of that feature's performance on user satisfaction, and the more important it is. In the plane with the satisfaction and dissatisfaction coefficients as two axes, the distance between the point representing the security feature $sf_j$ and the point of origin is taken as an indicator of the importance of the $sf_j$, calculated as: $Imp_j = \sqrt{SC_j^2 + DSC_j^2}$. In this way, the entire length of the questionnaire was effectively compressed without losing key information (Li and Xiao, 2020). The importance of security feature is further used as the proxy for the frequency of the cross-tabulation for correspondence analysis, since the higher the importance of a security feature is, it can be logically deduced that more people believe it to be important.

### 3.4. *Importance-satisfaction analysis*

Since Martilla and James (1977) first conduct market strategy induced by importance-performance analysis (IPA), the analytical method has been spread across a variety of industries such as computer, healthcare, tourism and retailing as a useful tool for customer satisfaction management (Hu et al., 2009) as well as identifying relative strengths and weaknesses of a company (Kuo et al., 2012). IPA uses the information collected to construct a matrix of two coordinates. In the IPA matrix, the horizontal axis represents the performance indicators of the object of analysis and the vertical axis represents its level of importance, where the median or the average of importance and performance are put in place of the slit of the matrix thus obtain four quadrants with different characteristics as follows.

(1) Keep up the good work: customer ratings of quality attributes in this quadrant are high in both performance and importance, so maintaining the high level of importance and performance is the strategy for quality attributes in this region.
(2) Concentrate here: customers have lower perceptions of performance but higher ratings of importance for quality attributes that are in this region. The strategy to this regional quality attributes is to focus on upgrading and refining them, with a gradual migration to quadrant "Keep up the good work".
(3) Low priority: Customer's perceived performance and importance of quality attributes in this quadrant are both low. It can be done without concern when resources are limited.
(4) Possible overkill: The quality attributes in this quadrant, which have high customer satisfaction and low perceived importance, are coped with by maintaining the high performance on the one hand, but with a relatively lower priority since their lower importance than that of quadrant "Keep up the good work", and on the other hand by increasing the perceived importance of customers by means of training or promotion to drift them towards quadrant "Keep up the good work".

However, through the previous analysis based on the Kano model, it can be concluded that the mechanisms by which the performance of different quality types of security features affect user satisfaction are different. The user's perception of satisfaction with two security features with exactly the same performance may be quite different, since on security feature may be "must-be" and the other a "attractive" one. While designers of smartphone security features are concerned with the user's perception of performance, it is far more important for them to understand the state of user satisfaction with security features. If a distinction is not made between performance and satisfaction and the two are used interchangeably, some confusions and ambiguities will be created. (Baker and Crompton, 2000; Oh, 2001). Tonge and Moore (2007) reconceptualized importance-performance analysis as importance-satisfaction analysis, while Wang (2016) provided an operationalization of importance-satisfaction analysis in conjunction with the Kano model.

Followed by these works, this study conducts importance-satisfaction analysis for smartphone security features to elicit strategies for designing and providing these features. In the previous section, the importance $Imp_j$ of security feature $sf_j$ was calculated through satisfaction coefficient $SC_j$ and dissatisfaction coefficient $DSC_j$, while performance of security feature $sf_j$ , denote as $Perf_j$, was also obtained through questionnaires. $Perf_j$ takes the average of all respondents' ratings and is normalized to between zero and one. Then the quantitative degree of satisfaction $Sat_j$ of $sf_j$ is calculated as:

$$Sat_j = Perf_j \cdot SC_j - (1 - Perf_j) \cdot DSC_j$$

From the formula, a completely fulfilled performance can result in satisfaction on the level of $SC_j$ while a performance totally unfulfilled can lead the satisfaction to be $-DSC_j$. In this study, the four quadrant names of the importance-satisfaction analysis remain consistent with the IPA, but the relationship between importance and satisfaction rather than performance is inscribed, which, as analyzed above, is argued to be more reasonable and closer to the original intent of the smartphone security designers.

## 4. Implementation

In this section, an industrial case is presented to demonstrate the implementation process as well as the results of our proposed analytical methods for understanding the asymmetric perceptions of security features for smartphones.

### 4.1. Data collection

The questionnaire was designed as shown in Table 2, mainly capturing the demographic characteristics of the respondents, operating system of smartphone, as well as the perceived quality and perceived performance of the security features of smartphones. The survey was conducted online. URL links to the questionnaire are distributed on instant messaging software and social media sites. In order to get sufficient feedbacks from developers and iOS users, the link to the questionnaire was also posted in mobile developer communities and Apple smartphone forums. A total of 268 questionnaires were collected, and after removing the missing-information and careless questionnaires, 245 samples were used for formal analysis, which included 92 developers and 153 smartphone users. The demographic characteristics of the 153 users are displayed in Table 4. According to "The 45th China Statistical Report on Internet Development" published by China Internet Network Information Center in April 2020 (CNNIC, 2020), the male to female ratio of Chinese Internet users is 51.9 to 48.1; 20–29 years old and 30–39 years old groups account for the highest percentage, with income of 3001–5000 CNY, 5001–8000 CNY and over 8000 CNY being the three groups with the highest proportion, which is basically consistent with the distribution characteristics of the sample in this study.

### 4.2. Results

#### 4.2.1. Perception of performance

Respondents' perceptions to the performance of the security features are measured directly in the questionnaire, and the sample group is divided as developers and users, while users are further subdivided into male and female, and iOS and Android users. The aggregated result of performance ratings for each security feature within each sample group are shown in Table 5.

**Table 4**
Demographic characteristics of users.

| Demographic variables | | Count | Percentage |
|---|---|---|---|
| Gender | Male | 85 | 55.6% |
| | Female | 68 | 44.4% |
| Age | <20 | 11 | 7.19% |
| | 20–29 | 52 | 34.0% |
| | 30–39 | 47 | 30.7% |
| | 40–49 | 24 | 15.7% |
| | >50 | 19 | 12.4% |
| Education | Junior high school or below | 24 | 15.7% |
| | High school | 36 | 23.5% |
| | Bachelor's degree | 62 | 40.5% |
| | Master's degree or higher | 31 | 20.3% |
| Personal income per month | None | 9 | 5.9% |
| | ≤CNY 1499 | 14 | 9.2% |
| | CNY 1500–2999 | 27 | 17.6% |
| | CNY 3000–4999 | 31 | 20.3% |
| | CNY 5000–7999 | 40 | 26.1% |
| | ≥CNY 8000 | 32 | 20.9% |
| Smartphone usage experience | <2 year | 30 | 19.6% |
| | 3–6 years | 51 | 33.3% |
| | 7–10 years | 42 | 27.5% |
| | >10 years | 30 | 19.6% |
| Operation system | iOS | 72 | 47.1% |
| | Android | 81 | 52.9% |

The results are also presented in Fig. 3 for a more intuitive comparison.

The performance of these 14 security features was averaged at 5.6, indicating that respondents were not very satisfied with the performance of current smartphone security features in general. There are large differences in performance scores for different security features. Among the high scoring security features are "Mobile Phone Anti-theft", "Battery Management", "Scanning Virus and Trojans", whereas low-performance security features include "URL and QR Code Security", "System Restoration and Rescue", "App Encryption and Lock" and "Data Backup". This provides an overall view of respondents' perceptions of performance across security features in aggregate. However, after distinguishing between different sample groups it is found that contributions to the overall performance are different for different subgroups of respondents, and some even vary considerably, although different subsamples tend to evaluate each security feature in a relatively consistent manner. For example, the performance rating for "Data Backup" security feature is 4.8 for males but only 2.9 for females, and 6.2 and 4.7 for males and females respectively for "Network and Traffic Management". Overall, males (M = 5.93) rate the performance of security features slightly higher than females (M = 5.58). Differences in users' perceptions of performance are likewise present across different operating systems. For instance, iOS users rate the performance of "App Permission Management" security features a 7.7, but Android users only score 3.4, whereas iOS users rate "App Encryption and Lock" at only 2.6 while Android users have a 6.3 rating. Variations in the perceived quality of security features also exist between ordinary users and developers: users give "Wi-Fi Security" features to 6.3 out of 10, while developers rate it only 4.1; users rate the security feature "Fraud and Harassment Prevention" a moderate 6.6, but developers give a higher rating of 7.9.

### 4.2.2. *Quality classification of security features*

Based on each respondent's Kano two-way questionnaire score for each security feature, the typical quality classification judgment of each respondent for each security feature can be determined according to the Kano typical quality classification table shown in Table 3. The aggregated frequency of typical quality classifications for all respondents is presented in column "Typical quality distribution" in Table 6. The typical quality type with the highest number of frequencies is designated as the traditional Kano type for a certain security feature. It can be seen from Table 6 that, similar to previous studies (Bu and Park, 2016; Yao et al., 2018), all the traditional Kano types for the 14 security features are "Indifferent" or "One-dimensional", which is not conducive to subsequent analysis. The improved Kano quality classification method, as described in Section 3.2, determines the final quality type by calculating the satisfaction and dissatisfaction coefficients for each security feature. The final Kano type results in Table 6 demonstrate that the 14 smartphone security features are distributed among four different Kano types. The "Attractive" security features include "Mobile Phone Anti-theft" and "System Restoration and Rescue". "One-dimensional" features include "Scanning Virus and Trojans", "App Permission Management", "Network and Traffic Management", "Wi-Fi Security" and "URL and QR Code Security". "Fraud and Harassment Prevention", "Malware Prevention" and "Cache and Garbage Cleanup" are "Must-be" features while "Banking and Payment Security", "App Encryption and Lock", "Battery Management", and "Data Backup" are determined as "Indifferent". Fig. 4 graphically presents the results of the Kano quality classification of the security features.

Not only do respondents have different perceptions of performance for different smartphone security features, but even for the same security feature, different respondents have different perceptions of quality. Smartphone security features are designed and implemented by security technology developers based on user needs, and there is a lack of testing in extant studies as to whether there is a gap between this conceived quality need and the real quality need of the user. For this purpose, the full sample is divided into developer and ordinary user groups, and the Kano quality classification is performed within each group to reveal the differences in developers' and users' perceptions of the quality of smartphone security features. The result is shown in Fig. 5. Interestingly, half of the 14 security features obtain with different Kano quality type across subsamples. For example, developers consider "Malware Prevention" and "Fraud and Harassment Prevention" to be "Must-be" qualities, while "URL and QR Code Security" and "Scanning Virus and Trojans" as "Attractive" qualities, but users classify them as "One-dimensional". Similar subgroup comparisons can be performed on different subsamples of users, so as to capture differences in the perceived quality of users of different genders, operating systems, etc.

**Table 5**
Respondents' perceptions to performance of security features.

| SAs | Details | Developer | User | | | | | All Average |
|---|---|---|---|---|---|---|---|---|
| | | | Male | Female | iOS | Android | Average | |
| BPS | Banking and Payment Security | 6.2 | 7.3 | 7.2 | 8.2 | 6.4 | 7.2 | 6.8 |
| FHP | Fraud and Harassment Prevention | 7.9 | 6.3 | 5.3 | 4.1 | 7.4 | 5.9 | 6.6 |
| MP | Malware Prevention | 6.6 | 6.8 | 7.6 | 9.3 | 5.3 | 7.2 | 7.0 |
| SVT | Scanning Virus and Trojans | 7.7 | 6.9 | 6.7 | 5.8 | 7.7 | 6.8 | 7.1 |
| AEL | App Encryption and Lock | 4.4 | 4.9 | 4.2 | 2.6 | 6.3 | 4.6 | 4.5 |
| APM | App Permission Management | 4.9 | 5.3 | 5.6 | 7.7 | 3.4 | 5.5 | 5.2 |
| MPA | Mobile Phone Anti-theft | 8.5 | 7.4 | 6.8 | 8.4 | 6.0 | 7.1 | 7.6 |
| NTM | Network and Traffic Management | 6.7 | 6.2 | 4.7 | 4.3 | 6.7 | 5.6 | 6.0 |
| WS | Wi-Fi Security | 4.1 | 6.1 | 6.6 | 7.0 | 5.7 | 6.3 | 5.5 |
| BM | Battery Management | 7.3 | 7.4 | 7.6 | 6.8 | 8.1 | 7.5 | 7.4 |
| DB | Data Backup | 5.4 | 4.8 | 2.9 | 2.6 | 5.1 | 3.9 | 4.5 |
| CGC | Cache and Garbage Cleanup | 6.8 | 6.5 | 5.2 | 4.2 | 7.5 | 6.0 | 6.3 |
| UQCS | URL and QR Code Security | 3.0 | 3.5 | 4.0 | 4.5 | 3.0 | 3.7 | 3.4 |
| SRR | System Restoration and Rescue | 4.8 | 3.6 | 3.9 | 4.8 | 2.8 | 3.8 | 4.1 |

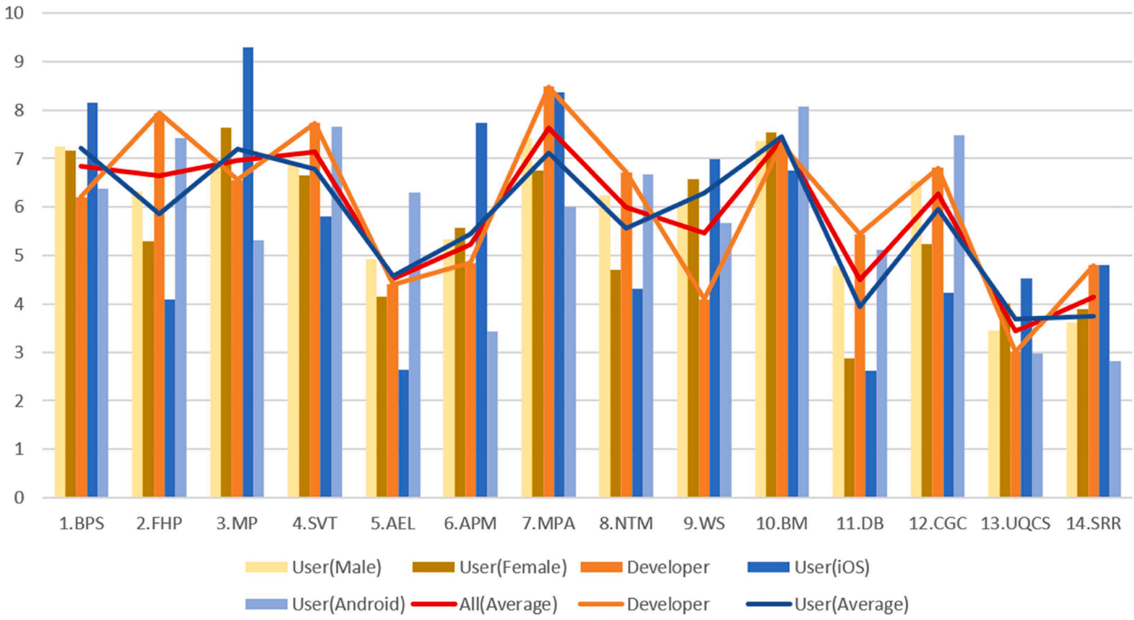


**Fig. 3.** Comparison of performance perceptions between sample groups.

**Table 6**
Kano-based analysis of security features.

| SAs | Typical quality distribution | | | | | | Tradition Kano Type | SC | DSC | Final Kano Type | Importance |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | A | M | O | I | R | Q | | | | | |
| BPS | 20 | 34 | 70 | 114 | 2 | 5 | I | 0.378 | 0.437 | I | 0.578 |
| FHP | 18 | 46 | 91 | 80 | 4 | 6 | O | 0.464 | 0.583 | M | 0.745 |
| MP | 14 | 38 | 97 | 87 | 3 | 6 | O | 0.470 | 0.572 | M | 0.741 |
| SVT | 27 | 30 | 89 | 90 | 1 | 8 | O | 0.492 | 0.504 | O | 0.704 |
| AEL | 18 | 22 | 82 | 112 | 1 | 10 | I | 0.427 | 0.444 | I | 0.617 |
| APM | 28 | 32 | 89 | 83 | 2 | 11 | O | 0.504 | 0.522 | O | 0.725 |
| MPA | 37 | 22 | 88 | 93 | 0 | 5 | I | 0.521 | 0.458 | A | 0.694 |
| NTM | 27 | 31 | 93 | 83 | 2 | 9 | O | 0.513 | 0.530 | O | 0.737 |
| WS | 36 | 31 | 89 | 78 | 2 | 9 | O | 0.534 | 0.513 | O | 0.741 |
| BM | 26 | 20 | 77 | 109 | 3 | 10 | I | 0.444 | 0.418 | I | 0.610 |
| DB | 20 | 19 | 89 | 103 | 2 | 12 | I | 0.472 | 0.468 | I | 0.664 |
| CGC | 25 | 34 | 89 | 89 | 2 | 6 | I/O | 0.481 | 0.519 | M | 0.708 |
| UQCS | 25 | 24 | 100 | 87 | 3 | 6 | O | 0.530 | 0.525 | O | 0.746 |
| SRR | 32 | 22 | 91 | 93 | 3 | 4 | I | 0.517 | 0.475 | A | 0.702 |

### *4.2.3. Correspondence analysis*

The results of the perceived importance for smartphone security features are presented in the last column of Table 6. “URL and QR Code Security”, “Fraud and Harassment Prevention”, “Wi-Fi Security”, “Malware Prevention”, and “Network and Traffic Management” are among the relatively important security features. After conducting chi-square test to ensure sufficient data variations, the results of the correspondence analysis presented in Figs. 6 and 7 depict the relationship between respondents’ perceptions of the importance of different security features across different groups.

As indicated by Fig. 6, “Network and Traffic Management”, “Cache and Garbage Cleanup” and “Wi-Fi Security” are perceived as highly important for developers, “System Restoration and Rescue” and “Banking and Payment Security” are favored by male users, while female users are more relevant to “Data Backup” than the others. Fig. 7 reveals that “Cache and Garbage Cleanup” and “Wi-Fi Security” are also relevant to developers. Android users’ perceptions of importance to “Scanning Virus and Trojans” are high, while “Data Backup”, “Malware Prevention”, “System Restoration and Rescue” and “URL and QR Code Security” are favored by iOS users.

### *4.2.4. Importance-satisfaction analysis*

In effort to understand the route the smartphone security strategy designer to follow to foster user satisfaction on smartphone securities, according to the method described in Section 3.4, an importance-satisfaction analysis was performed on the sample data and the results are shown in Fig. 8. Four different strategies are thus tailored to each of the 14 security features. In the “Keep up the good

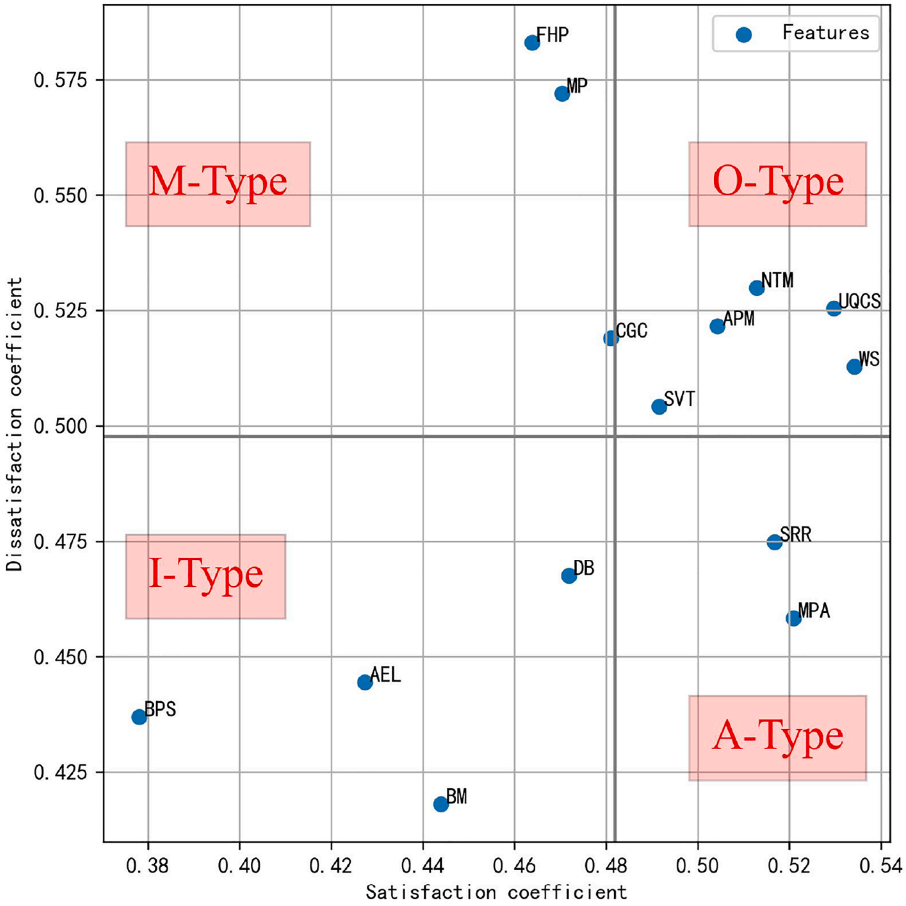


**Fig. 4.** Kano type plot of all samples.

work" quadrant, there locate security features "Fraud and Harassment Prevention", "Network and Traffic Management", "Malware Prevention", "Cache and Garbage Cleanup", "Scanning Virus and Trojans" and "Mobile Phone Anti-theft". These features are considered important and at the same time the users are satisfied with their performance. Thus they are in an ideal state and the future should try to maintain their high level of perceptions by users. The "Concentrate here" quadrant includes three security features as "URL and QR Code Security", "App Permission Management" and "System Restoration and Rescue". Users consider these security features important to them, but unfortunately current smartphones do not offer a satisfactory level of implementation and users are not satisfied with their performance. The next phase is to cater to user appetites and work to improve the performance of these security features to advance to the "Keep up the good work" quadrant. "Data Backup" and "App Encryption and Lock" are allocated in the "Low priority" quadrant. Although they do not have a high level of user satisfaction, they are not important features. Compared to the 10 security features mentioned earlier, the development priorities and attentions of these two features can be at a low level, especially when there are insufficient design and development resources to be allocated. The fourth quadrant is "Possible overkill", which include security features of "Battery Management" and "Banking and Payment Security". Users are satisfied with their performance, so they can be given a lower development priority while maintaining their higher performance, or they can be encouraged to raise the perception of their importance through security awareness and education, for example to emphasize the importance of bank account and payment security to users in the shopping and payments involved scenarios.

Also, by conducting importance-satisfaction analysis separately for different sample groups, the results shown in Table 7 are obtained. The results show that the quadrant composition is generally consistent across the different sample groups. However, there also exist differences between the different subgroups. For example, security features that developers have in mind to adopt a retention strategy include "Fraud and Harassment Prevention", "Network and Traffic Management" and "Cache and Garbage Cleanup", but users felt that "Fraud and Harassment Prevention" and "Network and Traffic Management" should be paid more attention by designers, while the high performance of "Cache and Garbage Cleanup" is not appreciated by users. A similar dislocation also exists between male and female users, as well as between iOS users and Android users, but to a much weaker extent. Such an importance-satisfaction analysis across sample groups is an important guide for smartphone security policy designers to accurately capture user segmentation needs and reallocate design resources.

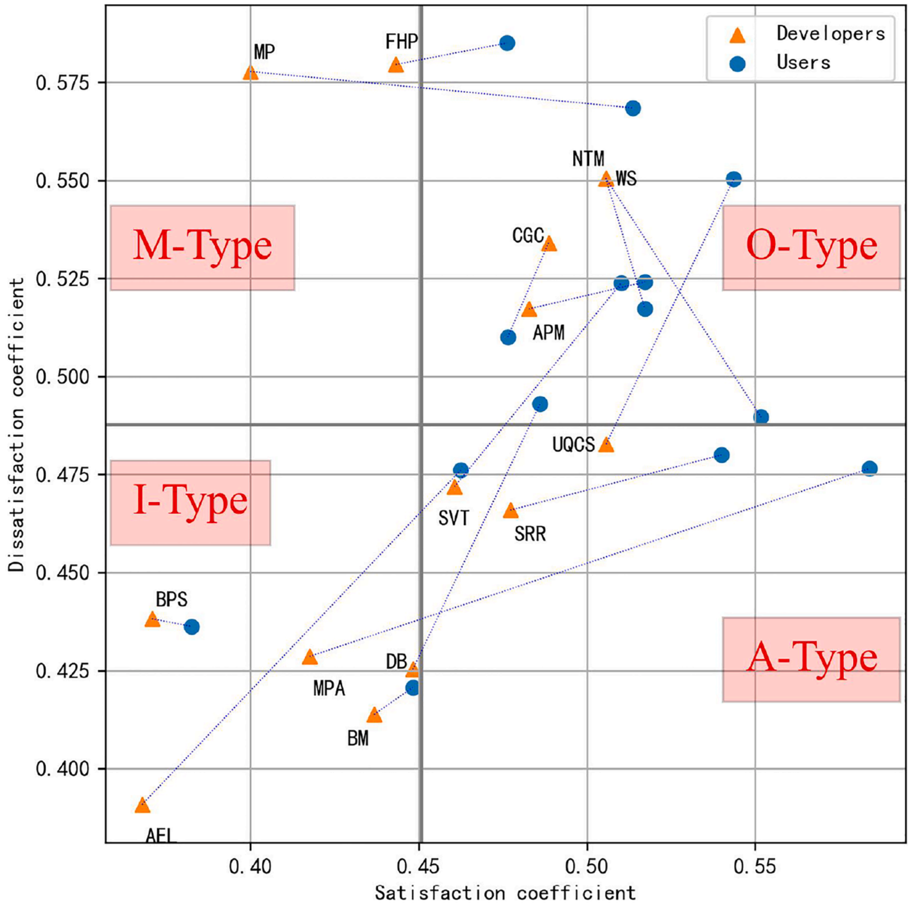


**Fig. 5.** Comparison of Kano type between users and developers.

## 5. Discussions and implications

### 5.1. Discussions

Smartphones provide a range of means to safeguard user privacy and data security, and 14 security features are extracted for investigation in this study. Within the framework of the research methodology presented in this paper, several interesting findings are obtained through the analysis of 245 questionnaires. Firstly, users' perceptions of the performance of different security features of current smartphones vary considerably, the average score tops out at 9.3 (iOS users for "Malware Prevention"), but the lowest score is only 2.6 (iOS users for "App Encryption and Lock"). Such differences in perceived performance exist between operating systems, between genders, and between developers and users. Overall, males rated their performance slightly higher than females on all security features, which may be due to the fact that males are more familiar with security-related technologies and their operations than females (Yao, et al., 2018), for example, females rated "Data Backup" and "Network and Traffic Management" lower than males. iOS users rate their performance on "App Permission Management" higher than Android users, which is related to iOS's unified and strict App permission management mechanism (Wang et al., 2013), but iOS users rate "App encryption and lock" lower than Android, which may be due to the fact that many customized Android-based systems provide individual encryption and locking permissions for Apps to help improve users' security and privacy appraisal (Subhash, 2020). Users and developers also differ in their performance evaluations of security features, for example, users score higher on "Wi-Fi Security" than developers, but lower on "Fraud and Harassment Prevention" than developers, which to some extent reflects the asymmetry between the perceptions of technology providers and demanders on the performance of the technology itself, and the identification of this asymmetry helps technology developers to provide more responsive functionality to the needs of users.

Second, the results of the analysis based on the improved Kano model suggest an asymmetry in users' perceptions of the quality of smartphone security features, with 14 security features distributed across attractive, one-dimensional, must-be, and indifferent quality (in Fig. 4), and the different Kano quality types reflect the difference in the degree to which unit performance improvement increases or decreases user satisfaction. A comparison of Kano types for users and developers shows that half of the security features achieved different quality categories (in Fig. 5), which is a noteworthy finding. Take "Fraud and Harassment Prevention" as an illustration, the

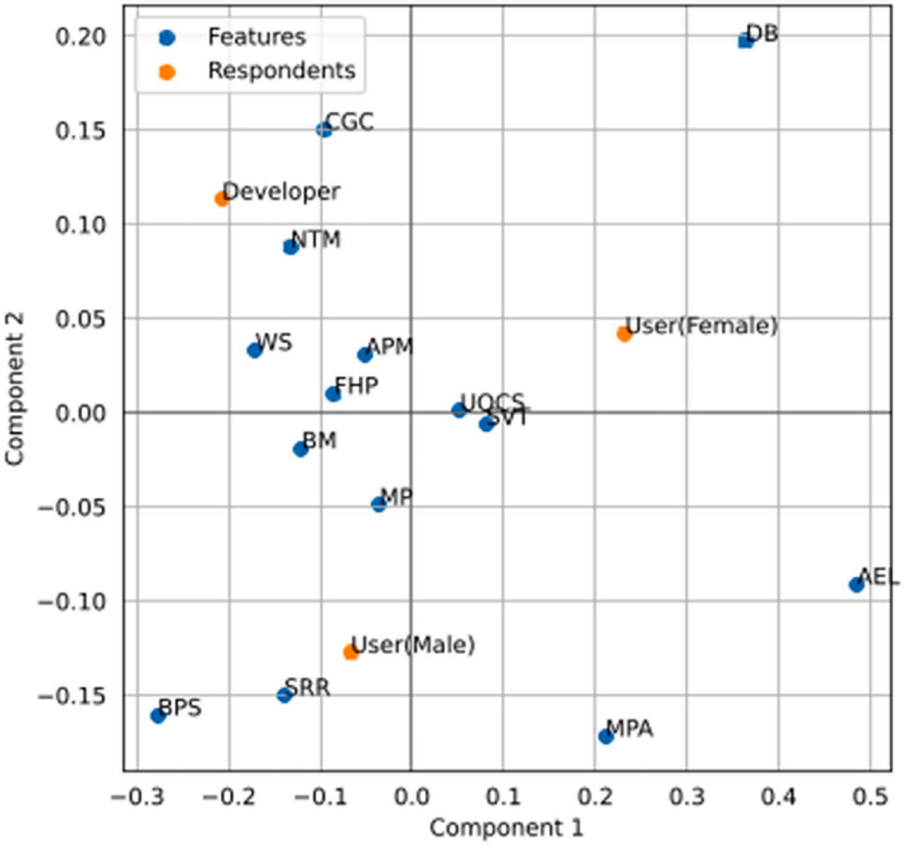


**Fig. 6.** Correspondence analysis (Developer, male user and female user).

users perceive it as one-dimensional quality, i.e., there is a approximatively linear relationship between performance and satisfaction, but the developers perceive as must-be quality, so when the developers value its performance to be above a certain satisfactory level, they may stop continuing to improve the performance because of the insignificant impact on user satisfaction. However, when considering in conjunction with the developers' and users' performance ratings of the "Fraud and Harassment Prevention" feature, which were 7.9 for developers and 5.9 for users, the overestimation of the performance of must-be security feature by developers may have resulted in greater harm to the user experience due to inertia towards improvement. These valuable findings have rarely been addressed in previous studies.

Third, asymmetries in users' perceptions of the importance of smartphone security features are effectively identified through the employment of correspondence analysis. The importance that users place on security features is tied both to the characteristics of the smartphone they use and to their own traits. The results indicate that male users attach more importance to "System Restoration and Rescue" and "Banking and Payment Security" features, which may be attributed to the fact that recovering and rescuing smartphones is largely done by men, who usually hold large sums of money or complete some large transactions, and are therefore more concerned about their bank account and payment security. Female users are more concerned about "Data Backup", probably because women are not good at backing up their data, so they expect smartphones to be convenient for supporting. Developers consider "Network and Traffic Management" and "Wi-Fi Security" to be more important, perhaps reflecting their worries about current status of smartphone network security. Android users are more focused on "Scanning Virus and Trojans" because they suffer from more virus and Trojans interference (Ahmad et al., 2013), whereas iOS users are more enthusiastic about features such as "Data Backup" and "System Restoration and Rescue", for example, many users report that the Apple's iTunes tool is unwieldy (Gordon, 2020).

Fourthly, the results of the ISA show that different prioritization strategies can be adopted for the optimization and resource allocation of different security features of smartphones. Fig. 8 and Table 7 show the detailed recommendations. In addition, comparisons between different sample groups emerged some valuable discoveries. For instance, there is a tendency for overly optimistic estimates of "Fraud and Harassment Prevention" and "Network and Traffic Management", which users believe should be of concern, but which developers believe can be maintained as is. There are gender differences in user claims for security features, which are largely manifested by variations in usage preferences and technical proficiency among users of different genders. Male users feel that "Network and Traffic Management" can be kept as status quo, but female users think it needs attention, probably because women prefer multimedia content with attractive visual display (Chrysostomou et al., 2009), such as music, pictures and video streams, which consume a large amount of network traffic. Additionally, male users regard the "Cache and Garbage Cleanup" feature as over-

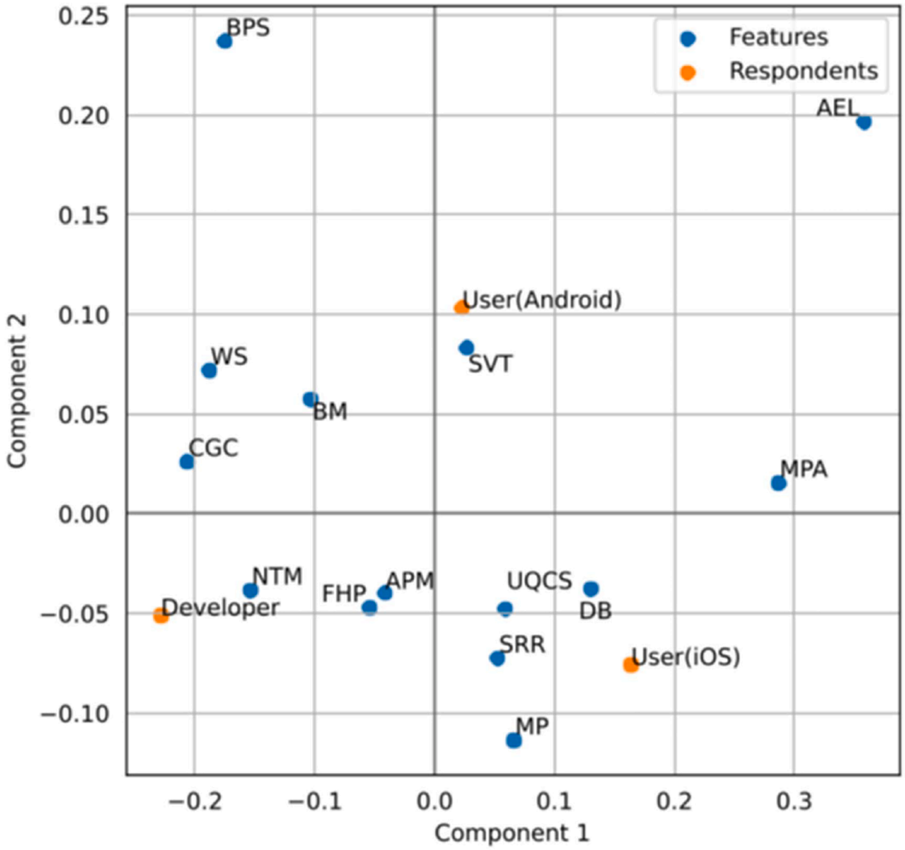


**Fig. 7.** Correspondence analysis (Developer, iOS user and Android user).

performing, but female users are more aware of it, presumably because women are less technically proficient and less savvy about how cache and garbage cleanup is handled. The differences between iOS and Android systems are also present. In addition to the differences mentioned previously, the results show that for “System Restoration and Rescue” security feature, iOS users perceive a need for attention but are a low priority for Android users, possibly owing to that Android devices are generally cheaper (Wukkadada et al., 2015), and data can be easily accessed using a USB cable or an external SD card to export (Elva, 2020), with many swiping tools available to support the restoration and rescue (Tan et al., 2018), whereas iphones are generally more expensive, with a more closed system and higher cognitive and financial costs of repair and rescue, and hence more emphasized by users.

### 5.2. *Implications*

This study yields a wealth of insights both theoretically and practically. On the theoretical side, this paper firstly examines smartphone security at the microscopic feature level and identifies 14 security features, which provide a more systematic and comprehensive foundation for subsequent research on smartphone security. Secondly, the results of the traditional Kano model for classifying quality attributes were unsatisfactory, and the problem of including only “Indifferent” and “One-dimensional” types of quality was also present in the current study. The improved Kano classification method proposed in this paper is able to better address this classification bias of traditional models, with which the 14 security features are assigned to each of the four categories: “Attractive”, “Must-be”, “One-dimensional”, and “Indifferent”. The different Kano categories reflect the different quality perception patterns of users, i.e. the different relationships between performance and satisfaction. Thirdly, the asymmetric perceptions of the importance of security features are captured by the intuitive approach, correspondence analysis. This paper endeavors to integrate the Kano model with correspondence analysis by taking importance as a frequency proxy, which is able to reuse the perceived importance information implicit in Kano questionnaire data and effectively compress the number items in the questionnaire. Fourthly, traditional importance-performance analysis focuses on the user’s rating of the performance of the evaluated object, but Kano model reveals a non-linear relationship between performance and user satisfaction, therefore, this study extends importance-performance analysis to importance-satisfaction analysis, which can more accurately profile smartphone users’ real perceptions of satisfaction with security features, and the results are more informative. Lastly and most importantly, the original aim of this study is to focus on the possible asymmetric perceptions of smartphone security features among different stakeholders, and to compare asymmetries throughout the text, making it one of the first studies to focus comprehensively on asymmetries in smartphone security. Lastly and most importantly,

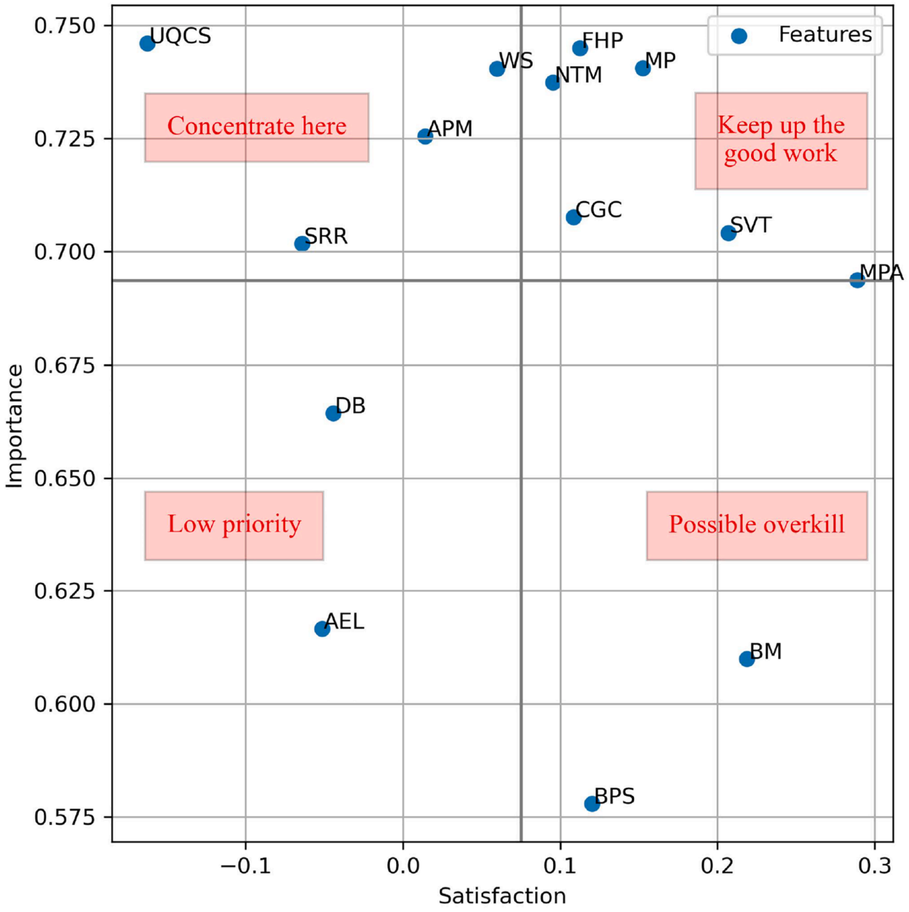


**Fig. 8.** Importance-satisfaction plot.

**Table 7**
Results of importance-satisfaction analysis across subsamples.

| Type | All | Developer | User | | | | |
|---|---|---|---|---|---|---|---|
| | | | Overall | Male | Female | iOS | Android |
| Keep up the good work | FHP, MP, SVT, MPA, NTM, CGC | FHP, NTM, CGC | MP, SVT, MPA, WS | MP, SVT, MPA, NTM, WS | MP, SVT, MPA | MP, APM, MPA | FHP, SVT, MPA, NTM, WS, CGC |
| Concentrate here | APM, WS, UQCS, SRR | MP, APM, WS, UQCS, SRR | FHP, APM, NTM, UQCS, SRR | FHP, APM, UQCS, SRR | FHP, APM, NTM, DB, CGC, UQCS | FHP, NTM, UQCS, SRR | MP, APM, UQCS |
| Possible overkill | BPS, BM | SVT, MPA, BM | BPS, BM, CGC | BPS, BM, CGC | BPS, WS, BM | BPS, SVT, WS, BM | BPS, AEL, BM |
| Low priority | AEL, DB | BPS, AEL, DB | AEL, DB | AEL, DB | AEL, SRR | AEL, DB, CGC | DB, SRR |

the research was originally designed to focus deeply on the possible asymmetric perceptions of smartphone security features across different stakeholders, which are compared throughout the text, making the study one of the first to investigate comprehensively on the asymmetries of smartphone security. The perspective, methodology, and findings of this study shed light on theoretical research on smartphone security design from user standpoint.

On the other side, this study serves as a practical guide for smartphone security providers (SSPs), such as smartphone manufacturers, designers, and developers, on security-related policies, resource allocation, and optimization practices. This paper highlights the chasm between the availability of security features provided by SSPs and users' perception of risks, the objective existence of a large variety of risks and available security tools are underestimated or ignored by users, which can inspire SSPs' deeper introspection of the underlying explanations, and the 14 security features outlined provide a more comprehensive view and checklist for SSPs to analyze and solve the problem. The results of the analysis based on the improved Kano model prompt the SSPs that smartphone users perceive quality criteria differently across security features, and the findings of the correspondence analysis of perceived importance show that the association between different users and different design features varies considerably, while the importance-satisfaction analysis offers the directions of development that different security features can follow. By pointing out that multiple factors, including user demographic characteristics, usage preferences, and technology familiarity levels, should be taken into account when designing security policies, this work provides a more fine-grained practical guide for smartphone security designers than previous research. Smartphone security design is not a standard product on the assembly line, and personalized deliberation is a necessity.

## 6. Conclusions

Smartphones nowadays face a number of security issues, and despite various initiatives by smartphone manufacturers, security app developers, and researchers to improve smartphone security, consumers in general underestimate the threats. To dissect this issue exhaustively, this study explores potential asymmetries in smartphone users' perceptions of security features from a microscopic perspective, i.e. between security features, between users and developers, and between different user. In this paper, I propose a user perception-driven design science analytical framework to achieve the following research objectives: User perceptions of asymmetric quality of security features are captured with an improved Kano model; asymmetric perceptions of importance are identified using a proposed "importance as proxy of frequency" correspondence analysis; the development pathways that are appropriate for different groups with different security features are planned following an importance-satisfaction analysis.

Although this study has certain uniqueness in terms of perspective and method, and provide clear theoretical and practical implications, there are certain limitations, which provide possible topics for future research. First, data collection is done in China, and a single national data source does not guarantee generalizability of results across cultures, and if cross-cultural differences of user perceptions exist are not examined. Second, although this study attempts to compress the total length of the questionnaire by calculating the importance from the Kano questionnaire, the two-way questions of the Kano model tend to lead the total number of questions excessive. In the future, the use of objective data to capture smartphone users' perception of security features could be considered. Finally, in terms of user group segmentation, this study only considered gender and operation system. In the coming future other different user segmentation strategies, such as novice and veteran, as well as differentiation from the use context (Li and Siponen, 2011), such as at home or in the office, could be explored.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Acknowledgements

This work was partially supported by the grant of National Natural Science Foundation of China [No. 71861014, 71863015], China Postdoctoral Science Foundation [No. 2019M652272], China Social Science Foundation [No. 20ZDA047], Priority Postdoctoral Research Projects of Jiangxi Province [No. 2018KY10], the Science and Technology Project of Jiangxi Education Department [No. GJJ60458] and the Social Science Project of Jiangxi Province [No. 17BJ31].

## References

Ahmad M.S., Musa N.E., Nadarajah R., et al. Comparison between android and iOS Operating System in terms of security. The 8th International Conference on Information Technology in Asia (CITA), July, 2013, 1-4.

Alani, M.M., 2017. Android user privacy awareness survey. Int. J. Interact. Mobile Technol. 11 (3), 130–144.

Alavi, A.H., Buttlar, W.G., 2019. An overview of smartphone technology for citizen-centered, real-time and scalable civil infrastructure monitoring. Future Generation Comput. Syst. 93, 651–672.

Alazab, M., 2014. Analysis on smartphone devices for detection and prevention of malware. Doctor of philosophy thesis. Deakin University, p. 285.

Alazab, M., Alazab, M., Shalaginov, A., et al., 2020. Intelligent mobile malware detection using permission requests and API calls. Future Gener. Comput. Syst. 107, 509–521.

Ameen, N., Tarhini, A., Shah, M.H., et al., 2020. Employees' behavioural intention to smartphone security: a gender-based, cross-national study. Comput. Hum. Behav. 104, 106148.

Baker, D.A., Crompton, J.L., 2000. Quality, satisfaction and behavioral intentions. Ann. Tour. Res. 27 (3), 785–804.

Berger, C., 1993. Kano's methods for understanding customer-defined quality. Center Quality Manage. J. 2, 3–36.

Bhagavatula, C., Ur, B., Iacovino, K., et al., 2015. Biometric authentication on iphone and android: usability, perceptions, and influences on adoption. In proceedings of USEC.

Bonnington C., 2015. In less than two years, a smartphone could be your only computer. Retrieved 12 February 2020 from https://www.wired. com/2015/02/smartphone-only-computer.

Brandom R. There are now 2.5 billion active Android devices, 2019. Retrieved 2 May 2020 from https://www.theverge.com/2019/5/7/18528297/google-io-2019-android-devices-play-store-total-number-statistic-keynote.

Breitinger, F., Nickel, C., 2010. User survey on phone security and usage. BIOSIG 139–144.

Breitinger, F., Tully-Doyle, R., Hassenfeldt, C., 2020. A survey on smartphone user's security choices, awareness and education. Comput. Sec. 88, 101647.

Bu, K., Park, S.Y., 2016. Are consumers in collectivist culture mostly indifferent to sports lesson programs?: a DAQ simulation on the Kano fuzzy model. J. Business Res. 69, 1656–1660.

Cabalquinto, E., Hutchins, B., 2020. It should allow me to opt in or opt out": Investigating smartphone use and the contending attitudes of commuters towards geolocation data collection. Telem. Inform. 51, 101403.

Chang, C.C., Chen, P., Chiu, F., et al., 2009. Application of neural networks and Kano's method to content recommendation in web personalization. Expert Syst. Appl. 36, 5310–5316.

Chebyshev V., 2020. Mobile malware evolution 2019. Retrieved 4 May 2020 from https://securelist. com/mobile-malware-evolution-2019/96280/.

Chen, C.C., Chuang, M.C., 2008. Integrating the Kano model into a robust design approach to enhance customer satisfaction with product design. Int. J. Prod. Econ. 114, 667–681.

Chen, L., 2012. A novel approach to regression analysis for the classification of quality attributes in the Kano model: an empirical test in the food and beverage industry. Omega 40, 651–659.

Chin, E., Felt, A.P., Sekar, V., et al., 2012. Measuring user confidence in smartphone security and privacy. In proceedings of the eighteenth symposium on usable privacy and security.

Choi, J.H., Lee, H.J., 2012. Facets of simplicity for the smart phone interface: A structural model. Int. J. Human Comput. Stud. 70 (2), 129–142.

Chrysostomou, K., Chen, S.Y., Liu, X., 2009. Investigation of users' preferences in interactive multimedia learning systems: a data mining approach. Int. Learn. Environ. 17 (2), 151–163.

CNNIC., 2020. The 45th China Statistical Report on Internet Development. Retrieved 1 May 2020 from http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/202004/P020200428596599037028.pdf.

De Leeuw, L., Mair, P., 2009. Simple and canonical correspondence analysis using the R package anacor. J. Stat. Softw. 31 (5), 1–18.

Dini, G., Martinelli, F., Matteucci, I., et al., 2018. Risk analysis of android applications: A user-centric solution. Future Gener. Comput. Syst. 80, 505–518.

Doey, L., Kurta, J., 2011. Correspondence Analysis applied to psychological research. Tutor. Quantit. Methods Psychol. 7 (1), 5–14.

Elva. How to Backup Android to SD Card. Retrieved 24 July 2020 from https://toolbox.iskysoft.com/ backup-android/how-to-backup-android-to-sd-card.html.

Enck, W., Gilbert, P., Chun, B., et al., 2010. TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. Proc. Symp. Oper. Syst. Design Implem.

Fan, W., Narang, H., Clarke, D., 2014. An overview of mobile malware and solutions. J. Comput. Commun. 2, 8–17.

Farivar, F., Haghighi, M., Jolfaei, A., Alazab, M., 2020. Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber physical systems and industrial IoT. IEEE Trans. Ind. Inf. 16 (4), 2716–2725.

Faruki, P., Bharmal, A., Laxmi, V., et al., 2015. Android security: a survey of issues, malware penetration, and defense. IEEE Commun. Surv. Tutor. 17 (2), 998–1022.

Fedler, R., Schutte, J., Kulicke, M., 2013. On the effectiveness of malware protection on android: An evaluation of android antivirus apps. Tech. Report.

Felt, A.P., Egelman, S., Wagner, D., 2012. I've got 99 problems, but vibration ain't one: A survey of smartphone user's concerns. Proc. Second ACM Workshop Security Privacy Smartphone Mobile Devices 33–44.

Florez-Lopez, R., Ramon-Jeronimo, J.M., 2012. Managing logistics customer service under uncertainty: An integrative fuzzy Kano framework. Inf. Sci. 202, 41–57.

Gartner,, 2020. Worldwide Smartphone Sales Will Grow 3% in 2020. Retrieved 1 May 2020 from. https://www.gartner.com/en/newsroom/press-releases/2020-01-28-gartner-says-worldwide-smartphone-sales-will-grow-3—.

Gerhards, J., Anheier, H.K., 1989. The literary field: An empirical investigation of Bourdieu's sociology of art. Int. Sociol. 4 (2), 131–146.

Go, M., Kim, I., 2018. In-flight NCCI management by combining the Kano model with the service blueprint: A comparison of frequent and infrequent flyers. Tour. Manage. 69, 471–486.

Gordon W. Why Does Everyone Hate iTunes? Should I Be Using Something Else? Retrieved 24 July 2020 from https://lifehacker.com/why-does-everyone-hate-itunes-should-i-be-using-someth-1221209656.

Harbach, M., Hettig, M., Weber, S., et al., 2014. Using personal examples to improve risk communication for security & privacy decisions. In: In proceedings of the 32nd annual ACM conference on human factors in computing systems, pp. 2647–2656.

Hertlein, K., 2012. Digital dwelling: technology in couple and family relationships. Fam. Relat. 61 (3), 374–387.

Hoffman, D.L., Frank, G.R., 1986. Correspondence analysis: Graphical of categorial data in marketing research. J. Mark. Res. 23 (3), 213–227.

Hu, H., Lee, Y., Yen, T., et al., 2009. Using BPNN and DEMATEL to modify importance–performance analysis model – A study of the computer industry. Expert Syst. Appl. 36, 9969–9979.

Hussain, M., Zaidan, A.A., Zidan, B.B., et al., 2018. Conceptual framework for the security of mobile health applications on Android platform. Telem. Inform. 35, 1335–1354.

Ilbahar, E., Cebi, S., 2017. Classification of design parameters for E-commerce websites: a novel fuzzy Kano approach. Telem. Inform. 34, 1814–1825.

Imgraben, J., Engelbrecht, A., Choo, K., 2014. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. Behav. Inf. Technol. 33 (12), 1347–1360.

James, F.C., McCulloch, C.E., 1990. Multivariate analysis in ecology and systematics: panacea or Pandora's box? Annu. Rev. Ecol. Syst. 21, 129–166.

Jones, B.H., Chin, A.G., 2015. On the efficacy of smartphone security: a critical analysis of modifications in business students' practices over time. Int. J. Inf. Manage. 35 (5), 561–571.

Jorgensen, Z., Chen, J., Gates, C., et al., 2015. Dimensions of risk in mobile applications: a user study. In proceedings of the 5th ACM conference on data and application security and privacy.

Kano, N., Seraku, N., Takahashi, F., et al., 1984. Attractive quality and must-be quality. J. Japan. Soc. Quality Control 14 (2), 39–48.

Kim, M., Chang, Y., Park, M., et al., 2015. The effects of service interactivity on the satisfaction and the loyalty of smartphone users. Telemat. Inform. 32, 949–960.

Kopackova, H., Komarkova, J., 2020. Participatory technologies in smart cities: What citizens want and how to ask them. Telemat. Inform. 47, 101325.

Kraus, L., Wechsung, I., Moller, S., 2017. Psychological needs as motivators for security and privacy actions on smartphones. J. Inf. Sec. Appl. 34, 34–45.

Kraus, L., Wechsung, I., Moller, S., 2014. Using statistical information to communicate android permission risks to users. Workshop Socio-technical Aspects Security Trust 48–55.

Kuo, Y.F., Chena, J.Y., Deng, W.J., 2012. IPA-Kano model: a new tool for categorising and diagnosing service quality attributes. Total Quality Manage. Business Excellence 23 (7), 731–748.

La Polla, M., Martinelli, M., Sgandurra, F., 2013. A survey on security for mobile devices. IEEE Commun. Surv. Tutorials 15 (1), 446–471.

Lee, Y., Huang, S., 2009. A new fuzzy concept approach for Kano's model. Expert Syst. Appl. 36, 4479–4484.

Li, Y., Siponen, M., 2011. A call for research on home users' information security behaviour. PACIS 2011 Proceedings 112.

Li, S., Xiao, Q., 2020. Classification and improvement strategy for design features of mobile tourist guide application: A Kano-IPA approach. Mobile Inf. Syst. 8816130.

Lin, S., Yang, C., Chan, Y., et al., 2010. Refining Kano's 'quality attributes–satisfaction' model: A moderated regression approach. Int. J. Prod. Econ. 126, 255–263.

Liu, S., Xiao, W., Fang, C., Zhang, X., Lin, J., 2020a. Social support, belongingness, and value co-creation behaviors in online health communities. Telematics Inform. 50, 101398.

Liu, S., Zhang, M., Gao, B., Jiang, G., et al., 2020b. Physician voice characteristics and patient satisfaction in online health consultation. Inform. Manage. 57 (5), 103233.

Lofgren, M., Witell, L., 2008. Two decades of using Kano's theory of attractive quality: A literature review. Quality Manage. J. 15 (1), 59–75.

Lopez-Fernandez, O., Kuss, D.J., Romo, L., et al., 2017. Self-reported dependence on mobile phones in young adults: a European cross-culture empirical survey. J. Behav. Addict. 6 (2), 168–177.

Martilla, J.A., James, J.C., 1977. Importance-performance analysis. J. Market. 41 (1), 77–79.

Matzler, K., Hunterhuber, H.H., 1998. How to make product development projects more successful by integrating Kano's model of customer satisfaction into quality function deployment. Technovation 18 (1), 25–38.

Mishra, S., Soni, D., 2020. Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis. Future Gener. Comput. Syst. 108, 803–815.

Moller, A., Michahelles, F., Diewald, S., et al., 2012. Update behavior in app markets and security implications: a case study in google play. In: In proceedings of the 3rd International workshop on research in the large. held in conjunction with mobile HCI, pp. 3–6.

Mylonas, A., Kastania, A., Gritzalis, D., 2013. Delegate the smartphone user? Security awareness in smartphone platforms. Comput. Sec. 34, 47–66.

Newzoo,, 2019. Top Countries by Smartphone Users. Retrieved 21 April 2020 from https://newzoo. com/insights/rankings/top-countries-by-smartphone-penetration-and-users/.

Oh, H., 2001. Revisiting importance-performance analysis. Tour. Manage. 22, 617–627.

Oldenburg R., 2015 Pushbullet updated for Android 6.0 (Marshmallow). Retrieved 6 May 2020 from https://blog.pushbullet.com/ 2015/11/03/pushbullet-updated-for-android-6-marshmallow/.

Qamar, A., Karim, A., Chang, V., 2019. Mobile malware attacks: review, taxonomy & future directions. Future Gener. Computer Syst. 97, 887–909.

Siponen, M., 2002. Designing secure information systems and software: Critical evaluation of the existing approaches and a new paradigm. University of Oulu.

Srinivas, J., Das, A.K., Kumar, N., 2019. Government regulations in cyber security: Framework, standards and recommendations. Future Gener. Computer Syst. 92, 178–188.

Subhash D. How to Lock Apps on Android. Retrieved 24 July 2020 from https://www.it4nextgen.com/app-lock-android/.

Tan, Y., Xue, Y., Liang, C., et al., 2018. A root privilege management scheme with revocable authorization for Android devices. J. Network Comput. Appl. 107, 69–82.

Ting, S.C., Chen, C.N., 2002. The asymmetrical and nonlinear effects of store quality attributes on customer satisfaction. Total Quality Manage. 13 (4), 547–569.

Tonge, J., Moore, S.A., 2007. Importance-satisfaction analysis for marine-park hinterlands: A Western Australian case study. Tour. Manage. 28 (3), 768–776.

Tontini, G., 2007. Integrating the Kano model and QFD for designing new products. Total Quality Manage. 18 (6), 599–612.

Verkijika, S.F., 2018. Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. Comput. Security 77, 860–870.

Wang, D., Xiang, Z., Fesenmaier, D.R., 2014. Adapting to the mobile world: A model of smartphone use. Ann. Tour. Res. 48, 11–26.

Wang T., Lu K., Lu L., et al. Jekyll on iOS: When benign apps become evil. In: Proceedings of the 22nd USENIX conference on Security, Washington, DC, USA, August 14-16, 2013. Hrsg. von Samuel T. King. USENIX Association, 2013, S. 559-572.

Wang, X., Lee, K.M., 2020. The paradox of technology innovativeness and risk perceptions – A profile of Asian smartphone users. Telem. Inform. 51, 101415.

Wukkadada, B., Nambiar, R., Nair, A., 2015. Mobile operating system: analysis and comparison of android and iOS. Int. J. Comput. Technol. 2 (7), 273–276.

Yao, M., Chuang, M., Hsu, C., 2018. The Kano model analysis for features for mobile security applications. Comput. Sec. 78, 336–346.

Zaidi, S., Shah, M., Kamran, M., et al., 2016. A survey on security for smartphone device. Int. J. Adv. Comput. Sci. Appl. 7 (4), 206–219.

Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., Zhu, Q., 2018. Health information privacy concerns, antecedents, and information disclosure intention in online health communities. Inform. Manage. 55 (4), 482–493.

Zulkefli, Z., Singh, M.M., 2020. Sentient-based access control model: a mitigation technique for advanced persistent threats in smartphones. J. Inform. Sec. Appl. 51, 102431.

**Quan Xiao** is an Associate Professor in the School of Information Management, Jiangxi University of Finance and Economics. He received his Ph.D. in information systems from Huazhong University of Science and Technology. He holds Information Technology Project Management Professional and has been responsible for the design and development of more than ten information system projects. His research interests include the design of information systems and information security.