Exploring the User Security Experience of Mobile Payment in China

Jiaxin Zhang and Yan Luximon*
School of Design
The Hong Kong Polytechnic University
Hung Hom, Hong Kong
e-mails: jx.zhang@connect.polyu.hk, *yan.luximon@polyu.edu.hk

Abstract— **Mobile payment services are in widespread use in China, but with them come growing concerns about security. Although the security of mobile payment has been demonstrated, a sample of user experience derived from real world data must be collected to understand the complex use context. This study aims to contribute to the current research by providing qualitative data through in-depth semi-structured interviews. The research explores the user security experience in a variety of use contexts by investigating mobile payment services in a mature market. The findings showed that users view their security experience as composed both financial and privacy aspects. The key user experience for mobile payment security was divided into five components: online mobile transaction, in-store payment, peer-to-peer payment, payment interaction in the physical world, and the network environment. Useful elements were also identified for enhancing security experience for mobile payment. Investigating security experience and user needs when designing mobile payment systems in context will provide a more holistic picture of the security needs surrounding mobile payment.**

Keywords-mobile payment; security; user experience; use context.

I. INTRODUCTION

Advances in mobile technology have led to the increased popularity of mobile services in recent years. Mobile payment is vital to the development of mobile services, allowing for numerous diverse electronic transactions, such as online and offline purchasing, payment of bills and peer-to-peer transfer [1][2]. As China is one of the largest mobile payment markets in the world, it has drawn a great deal of attention from both practitioners and researchers [3]. According to the 40th China Statistical Report on Internet Development [4], there are 502 million mobile payment users in China. 90% of users (463 million) use mobile payment in offline situations, resulting in a variety of use contexts; these include payments made at physical stores, large retailers, vending machines, restaurants, hotels and public transportation. Mobile payment platforms, such as Alipay and WeChat Pay [5] have not only reduced the use of cash, but have also provided other supporting functions, including account and money management, location information and financial services, which enhance user experience while using mobile payment [2]. It is not surprising that mobile payment has become a part of everyday life in China. However, this widespread adoption has created multiple transaction scenes, leading to increasing security concerns in both the financial and privacy aspects [6][7].

This paper focuses on the security experience of mobile payment in a well-developed mobile services market, where various mobile payment scenarios can be identified and discussed. The purpose of this study is to investigate the specific user experiences of mobile payment to explore the associated factors and use contexts related to specific security experience. The study also tried to determine the user perspective of mobile payment security. The findings of this research could provide a comprehensive understanding of users' security needs in different mobile payment scenarios and past experiences of the users in a mature market of mobile payment. The following sections of this article are organized as follows: Section II introduces the state of the art in mobile payment and security research. Section III describes the method applied for the study. Section IV outlines the participants' demographic information and results of the interview. Section V compares the current results with previous research outcomes. Section VI presents the conclusion of the main findings and indicates the possible fields for future research.

II. STATE OF THE ART

Previous studies have found a strong relationship between perceived security of electronic commerce and user attitudes toward its adoption [7]-[9]. Research studies have reported that security risks have been an important factor influencing customer's willingness in using mobile payment in China [10]. Although this consumer "adoption" study has demonstrated the importance of mobile payment security, simply using "adoption" research to investigate the impact of mobile payment security might not be effective enough for evaluating the overall situation and gaining broader insights about this area [11].

With the increasing adoption of mobile services, researchers have emphasized on the importance of studying the relationship between use context and security of mobile payment. For instance, Figge [12] is concerned about information confidentiality regarding the context computation. Since consumer information is sent out for improving mobile services in different use contexts, service providers could access to a lot of personal information. Dahlberg et al. [11] have mentioned the research value of understanding use context and security in mobile payment, and suggested the need to map the use context of mobile payment with security methods, which can be regarded as a promising research area.

 ISBN: 978-1-61208-616-3

Today, the use context of mobile payment in China is more and more complex, as the platforms such as Alipay and WeChat Pay have created a mobile lifestyle rather than simply providing a service. This calls for studies to understand of security experience of mobile payment usage in a particular situation. As compared to provious empirical studies, interviews can help in collecting data regarding user attitude and experience regarding the daily use of mobile payment services in use contexts. This contributes to an overall understanding of the formation of security experience depending on the scenarios and provides insights for enhancing mobile payment interaction.

III. METHOD

Semi-structured in-depth interviews were adopted for this research to investigate the user security experience of mobile payment in order to form a holistic understanding of the phenomenon.

A. Participants

In order to identify the most cases across various payment scenarios, we conducted the research in a mature market to collect as much user experience as possible. We recruited 10 participants (5 male and 5 female users) in Guangdong province in China, where mobile payment services are widely used.

B. Interview Design

A semi-structured in-depth interview was conducted for each participant individually. Each interview ranged from 25 to 45 minutes, depending on the participant's experience in the topic. The interview was conducted either in person or by phone. Before the interview, each participant completed a questionnaire on their demographic information as well as their experience with using mobile payment, including the platforms they had used, the frequency and duration of use and the transaction amount per month. At the beginning of the interview, all participants were asked if they believe mobile payment is secure. Next, we asked participants about their security concerns when using mobile payment. The purpose of these two questions was to determine what users want to protect most when using mobile payment, thus allowing us to identify user concerns regarding mobile payment security more accurately. Participants were then required to think about previous secure or insecure experiences in different use contexts of mobile payment. Finally, the interviewer asked participants what factors they believed to influence their perception of security in mobile payment, and to identify their reasons. All interviews were recorded for data analysis.

C. Data Analysis

The coding method applied in this study is that of Strauss, which requires grounding to the data [13]. First, the voice data were transcribed to text. We examined the data, made notes and coded according to three themes: security concerns in mobile payment, security experience and use context and other elements related security experience. Labels and themes were developed based on each topic to create categories and generate theory.

IV. RESULTS

The findings that emerged from the interview are as shown. The results section presents a detailed explanation of how user security experience is formed, as well as the important elements that influence it.

A. General Information

The average age for participants is 25.6 years (SD=2.12; age range: 21-29). All participants had experience using mobile payment, such as WeChat Pay, Alipay, UnionPay Online, Apple Pay, Baidu Wallet, JD Pay, Tenpay, 99 Bill or Mobile Banking. 70% are customers with more than 3 years' experience using mobile payment; 20% are users with 1-3 years' experience; and 10% have less than 1 year of experience. The percentage of monthly expenditure through mobile payment ranges from 7.5% to 100% of their monthly income.

B. Security Concerns in Mobile Payment

All participants were asked at the beginning "*Do you think it is secure to adopt mobile payment service and what are your security concerns with it?*" 5 participants (50%) responded that they believe it is secure, while 4 participants (40%) believe it is insecure. 1 participant (10%) stated that it depends on the reputation of the service provider. 8 participants (80%) said that they considered both financial and privacy aspects; of these, 3 participants concluded that financial security was more important, 2 participants stated that information security was more essential, and 3 participants thought that financial and information security are equally important. 2 participants considered only one or the other of financial or information security. Surprisingly, 2 participants (20%) stated that they had few worries regarding potential financial loss, due to the small amounts of their transactions and high popularity of the mobile payment platform.

TABLE I. PRIVACY INFORMATION CONCERNS

Privacy Information concerns	
Privacy information	***Frequency***
Phone number	7
ID number	5
Consumption record	3
Address	2
Cookies	2
Account	1
Job information	1
Name	1
Financial information	1

According to the above responses, most participants emphasized the importance of their privacy. We explored the reasons for this with further questions, and 3 participants said it was because relationships can be traced through information. For example, they believe that a person's mobile

payment account could reflect a behavior pattern, or a dishonest browsing history might have a negative influence on their personal credit. Participants also mentioned the specific privacy information they would be reluctant to disclose, as shown in Table I.

C. Security experience and use context

This section describes the security experience mentioned by participants in the interview process in order to present a comprehensive picture of security in daily life. We explored the security experience of our participants mainly by asking "*In what situation do you use mobile payment service*" and requiring them to "*describe secure and insecure use contexts of mobile payment usage according to your own experience*". In the case of mobile payment platforms, such as WeChat Pay and Alipay, participants in our study indicated a variety of user experiences that structured their perception of the security of these systems. Based on our analysis, user experience can be divided into five payment situations: online mobile transaction, in-store payment, peer-to-peer payment, payment interaction in the physical world and network environment. Online transaction focuses on payment scenarios made entirely on a mobile device. In-store payment involves a face-to-face transaction between merchants and consumers, while peer-to-peer payment describes a transfer made between parties with relatively strong ties. Payment interaction in the physical world involves payment between users and machines in the public space, and the final category refers to users' selection of network environment for mobile payment.

1) Online mobile transaction: The major experiences with online mobile transaction are associated with online shopping. In this situation, participants responded with two security considerations. The first relates to payment system usability. A system that runs smoothly and can provide efficient feedback during a transaction is necessary to ensure a positive user security experience. The second user security experience derives from the reputation of the merchant or payment service developer. In the case of developer reputation (with 70% of participants' concern), participants mainly worried about the security of their information. In terms of merchant reputation (with 50% of participants' concern), most of participants worried about the quality of goods bought online. Of note, 2 participants stated that insurance for account security was provided by certain platforms, such as WeChat Pay, Alipay and JD Pay, which enhanced their perception of the security of the system.

We also asked our participants to compare the platforms they have used in order to further understand the relationship between user experience and reputation. Alipay and WeChat Pay are the most popular mobile payment platforms in China. 5 respondents (50%) stated their belief that both of them are secure, while 5 respondents (50%) perceived that their security levels are different. 3 respondents indicated that frequency of use of a platform influenced their perception of security, which could lead to their belief that either Alipay or WeChat Pay is securer. Another factor is the different brand images of Alipay and WeChat Pay. U2 participant explained, "*Alipay looks like a large platform with various kinds of merchants in it. I am afraid that my privacy will be stolen and my money is insecure… Compared with Alipay, WeChat Pay is a platform for transferring between friends…Also, I usually use WeChat to keep in touch with my friends. I prefer to use WeChat Pay in my daily life since it is convenient and secure.*"

2) In-store payment: In the context of the physical store, mobile payment systems enable consumers to pay by scanning a merchant's QR code or by having their account's QR code scanned by a merchant. In the first case, users scan a QR code provided by the merchant, then input the charge as well as a password to settle the payment (Figure 1). In the second case, merchants input the amount of money first, while the consumer provides their account's QR code for the merchants to scan (Figure 2). This second transaction can be settled without the user inputting a password. The security experience is formed through the interaction between merchant and customer, as well as the physical environment. 2 participants (20%) said they felt insecure when paying by having their QR code scanned by merchants. They worried that merchants would charge them an amount of money higher than the actual price; in addition, this method of payment does not require their password to pay. These factors decrease their perception of security.

In addition, 2 participants (20%) felt the physical environment could be a risk for mobile payment users. Since surveillance cameras are installed in public places, users cannot avoid being recorded every time they input their password. U9 gave a detailed description of the situation: "*There are surveillance cameras in supermarkets or banks. When I use mobile payment to pay in these places, I input my passwords in a hurry sometimes. The charging process needs to be quick, so I am not able to use my hand to cover it, or my phone screen is too large to cover. My password would be easy to record.*"

Figure 1. User scanning merchant's QR code for payment

Figure 2. Merchant scanning customer's QR code for payment

3) Peer-to-peer payment: One particular advantage of mobile payment is that it supports peer-to-peer transfer,

leading to the convenience of transaction between individuals. Peer-to-peer payment can occur between strangers, such as buying food at a kiosk or paying a taxi bill, or between friends, such as sharing a dining fee or sending "gift money" [14]. Specifically, 1 participant (10%) mentioned their belief that the method of transferring money within a chat group is secure, where sender and recipient already know each other. This method allows immediate feedback, as well. U2 added that transactions among friends provide a much more secure experience in terms of mobile payment. For this reason, the participant prefers to use WeChat Pay rather than Alipay for peer-to-peer payment, as WeChat is also a chat application. In the case of payment between strangers, the participant stated that it is better to pay using paper money than to use mobile payment at a kiosk, because this might avoid the privacy being stolen.

4) Payment interaction in the physical world: The adoption of mobile payment has encouraged the development of self-service equipment, such as ticket machines, vending machines and bike sharing. This allows transactions not only from person to person, but also between man and machine. In this study, however, we found particular concerns when participants interacted with these machines in the physical world, as the transaction context has become more complex.

This consideration is not only restricted to the user interface, but also applies to the physical environment. Mobile payment for bike sharing was mentioned by several participants. Currently, users can pay to share bikes in the city by scanning a QR code using a mobile payment system. Unlike the QR code scanning that happens between users in person, self-service payment in public places may pose more risks. One concern is about the legitimacy of QR codes (Figure 3). When a QR code is used for payment in a public place, it is possible for users to become involved in fraudulent activities. For example, 2 participants stated they cannot tell whether a QR code is the original or one pasted on by criminals in order to steal the users' money.

Figure 3. Scanning a bike-sharing QR code in a public place

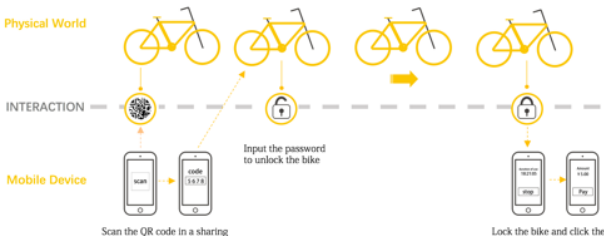

Figure 4. Payment settled in Mobike system

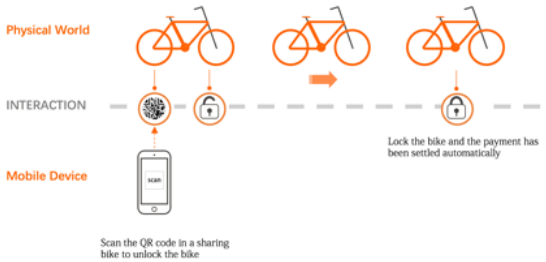

Figure 5. Payment settled in OfO system

Another concern is usability. Users have less experience when adopting a mobile payment system in a new context. The various payment processes across different services can cause an insecure experience. For example, in the bike-sharing system OfO, users must manually stop the charges after they return a bike, while Mobike (another bike-sharing system) stops charging the user automatically after returning a bike (Figure 4 and Figure 5). One participant worried that the manual system (OfO) might overcharge them if they forget to stop the charges after returning a bike. However, another participant thought the automatic system (Mobike) might secretly charge more than it should, as the system does not allow users to confirm the amount before payment is settled. This inconsistent process is likely to create an insecure experience, as users need more time to adapt to various payment processes despite the similar use context.

5) Network environment: Our research showed that participants are also concerned about the network environment when using mobile payment. 70% of participants emphasized that they would not use mobile payment on public Wi-Fi networks to avoid risk, while 5 participants (50%) said they would not connect to public Wi-Fi at all. It is clear that the mobile wireless network is a necessary trusted context for mobile transactions.

D. Other elements that relate to the security experience

In addition to user security experience, participants also mentioned other possible elements that influence the perceived security of mobile payment. 5 participants (50%) expressed the need for the customization of mobile payment platforms in order to improve their security experience. Different use contexts should be tailored to the particular user in terms of authentication methods for mobile payment. For instance, users require more complicate authentication methods (multi-factor authentication) to protect the payment of large transaction amount, while they want simpler methods to facilitate the payment of a small transaction amount. Participants also revealed that they are not being told what personal information is being disclosed by mobile payment platforms, but that they need to be made aware so that they can make choices that avoid disclosures of privacy. Another consideration is that designers need to think about users' capability of customizing the user interface. One participant said, *"If there are too many user settings, it will be a mess. I*

 ISBN: 978-1-61208-616-3

would be afraid that the device cannot run smoothly. Also, I will forget my settings."

What is interesting to note is that participants developed certain self-directed approaches to help themselves "feel more secure" when using mobile payment, such as hiding unfamiliar functions in the platform, regularly deleting records of mobile payment usage on their device, linking a credit card to their mobile payment user account or using two-step authentication on two different devices.

V. DISCUSSION

A. Security concerns

We investigated user concerns about security in mobile payment in both the financial and privacy aspect. As users connect with various kinds of services, including food take-out or delivery services, DiDi taxi, online and offline purchasing and social media, personal data is collected by mobile payment platforms to understand the particular user's behavior pattern and provide a more efficient service. A previous study revealed that social network services can expose user behavior patterns, known as privacy disclosure patterns [15]; our research found that users believe mobile payment platforms pose a similar risk to user privacy [16]. Based on the responses of our participants, a focus on intent to disclose private information through mobile payment, rather than concerns about financial losses, might have a more effective impact on user security experience. While some participants discussed the personal information they provided on mobile payment platforms, future research could investigate the importance of different types of personal data accessed by mobile payment systems and the possible consequence of privacy disclosure in mobile payment.

B. Weakening or strengthening user security experience

In examining the use context of mobile payment, we identified experiences that could strengthen or weaken perceived user security in particular situations. According to our participants' responses as well as the previous research [17], reputation is an important factor in the adoption of mobile commerce, especially in online shopping. A good reputation guarantees the security of possession and privacy. A readily available payment record will enhance the user's security experience, while delayed feedback or lack of information will weaken it. Regarding the payment process, participants added that when they pay without a password or have their codes scanned by a merchant to pay, they felt insecure. This is because they cannot confirm the transaction amount before the payment settled. These scenarios indicate that users expect to have better control over managing their accounts or the transaction process in order to enhance their security experience when using mobile payment. Unlike actual control, which refers to the capability of changing a situation, perceived control emphasizes the user's feeling of their ability to maintain a coming event [18]. Previous studies have demonstrated the importance of perceived control on security problems in other contexts [18][19]. The results presented in this study lead us to recommend more studies to investigate the influence of perceived control in mobile payment.

In addition, users felt more secure when money was transferred to their friends, rather than to strangers or merchants. Similar to the findings of a previous study [20], participants perceived the social relations in WeChat to be based on real life, while the social relations in Alipay are mostly based on virtual situations. The strong ties built in a user's actual life develop a sense of trustworthiness in mobile payment. According to previous studies [21], social influence can not only affect the user's intention of adopting mobile payment by enhancing its perceived usefulness, but also reducing user's perceived risk of mobile payment. The responses in this study reveal a relationship between social influence and perceived security in mobile payment.

C. The need for customization in the security experience

The interviews revealed the need for customization to enhance the security experience of mobile payment. Based on our results, setting authentication methods according to the use context holds the greatest attraction for participants. Authentication methods are a vital issue when it comes to the tradeoff between convenience and security in technology usage [22]. While customization of authentication methods is crucial for a positive security experience, use context is an important element. In this case, tailoring would occur according to "location, time or resources" [23]. The complex nature of mobile payment usage means designers must consider the extent to which users be given permission to customize the platform, in terms of the user's cognitive capabilities and the limitations of the mobile device. The creation of self-directed approaches in order to feel secure as reported by participants in the interviews may present possible solutions to this problem. Under this approach, a method of participatory design could be created to study the details for customization. Designers could learn from users' experience and knowledge, formed within the use context, in order to develop a comprehensive understanding of the users' needs [24].

VI. CONCLUSION AND FUTURE WORK

Although mobile payment has been adopted across many aspects of life in China, users have security concerns in different use contexts. In this study, we explored users' perspectives of mobile payment security in various use contexts, and discussed factors that could enhance user security experience. Through the interview process, we identified five use contexts for mobile payment to present a more holistic picture of mobile payment in China The study finding also recognized the need of design customization for improving the security. The result of this research could provide a reference to enhance security experience design according to users' needs and different use contexts in mature markets of mobile payment, while its effectiveness in developing markets of mobile payment will still require to be verified.

Future research on the user security experience of mobile payment can be focusing on determining what can be user security concerns in various payment scenarios and

 ISBN: 978-1-61208-616-3

categorizing their security experience for better experience design.

ACKNOWLEDGMENT

The authors would like to thank the support of the UGC Funding Scheme from the Hong Kong Polytechnic University.

REFERENCES

[1] L. Goeke and K. Pousttchi, "A scenario-based analysis of mobile payment acceptance," Mobile Business and 2010 Ninth Global Mobility Roundtable (ICMB-GMR), 2010 Ninth International Conference on, IEEE Press, Jun. 2010, pp. 371-378, doi: 10.1109/ICMB-GMR.2010.81

[2] T. Oliveira, M. Thomas, G. Baptista, and F. Campos, "Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology," Computers in Human Behavior, vol. 61, pp. 404-414, Mar. 2016, doi: doi.org/10.1016/j.chb.2016.03.030

[3] A. Y. L. Chong, "Understanding mobile commerce continuance intentions: an empirical analysis of Chinese consumers," Journal of Computer Information Systems, vol.53(4), pp. 22-30, Dec. 2015, doi: dx.doi.org/10.1080/08874417.2013.11645647

[4] CNNIC, the 40th China Statistical Report on Internet Development, 2017, http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201708/P020170807351923262153.pdf [retrieved: Feburary, 2018]

[5] iiMedia Research, The report for mobile payment market research of the first half year of 2017, retrieved from: http://www.iimedia.cn/53957.html [retrieved: Feburary, 2018]

[6] G. de Kerviler, N. T. M. Demoulin, and P. Zidda, "Adoption of in-store mobile payment: Are perceived risk and convenience the only drivers?" Journal of Retailing and Consumer Services, vol. 31, pp.334-344, May 2016, doi: doi.org/10.1016/j.jretconser.2016.04.011

[7] P. G. Schierz, O. Schilke, and B. W. Wirtz, "Understanding consumer acceptance of mobile payment services: An empirical analysis," Electronic commerce research and applications, vol. 9(3), Aug. 2009, pp. 209-216, doi: doi.org/10.1016/j.elerap.2009.07.005

[8] M. H. Shah, H. R. Peikari, and N. M. Yasin, "The determinants of individuals' perceived e-security: Evidence from Malaysia," International Journal of Information Management, vol. 34(1), Nov. 2013, pp. 48-57, doi: dx.doi.org/10.1016/j.ijinformgt.2013.10.001.

[9] C. Kim, W. Tao, N. Shin, and K. S. Kim, "An empirical study of customers' perceptions of security and trust in e-payment systems," Electronic commerce research and applications, vol. 9(1), Jun. 2009, pp. 84-95.

[10] W. Xu, "The Study of WeChat Payment Users Willingness Factor," Journal of Service Science and Management, vol. 10(3), Jun. 2017, pp. 251-259, doi: 10.4236/jssm.2017.103021

[11] T. Dahlberg, J. Guo, and J. Ondrus, "A critical review of mobile payment research," Electronic Commerce Research and Applications, vol. 14(5), Jul. 2015, pp. 265-284, doi: doi.org/10.1016/j.elerap.2015.07.006

[12] S. Figge "Situation-dependent services —a challenge for mobile network operators," Journal of Business Research, vol.57(12), Dec 2004, pp. 1416-1422, doi: doi.org/10.1016/S0148-2963(02)00431-9

[13] A. L. Strauss, Qualitative analysis for social scientists. Cambridge, UK: Cambridge University Press, 1987

[14] Y. M. Kow, X. Gui, and W. Cheng, "Special Digital Monies: The Design of Alipay and WeChat Wallet for Mobile Payment Practices in China," IFIP Conference on Human-Computer Interaction, Springer Press, Sep. 2017, pp. 136-155, doi: 10.1007/978-3-319-68059-0_9

[15] K. Li, Z. Lin, and X. Wang, "An empirical analysis of users' privacy disclosure behaviors on social network sites," Information & management, vol. 52(7), Jul. 2015, pp. 882-891, doi: dx.doi.org/10.1016/j.im.2015.07.006

[16] Y. Zhuang, A. C. M. Leung, and J. Hughes, "Matching in Proximity Authentication and Mobile Payment EcoSystem: What Are We Missing?" International Workshop on Radio Frequency Identification: Security and Privacy Issues, Springer Press, Jul. 2017, pp. 163-172, doi: 10.1007/978-3-319-62024-4_12

[17] K. Siau and Z. Shen, "Building customer trust in mobile commerce," Communications of the ACM, vol. 46, Apr. 2003, pp. 91-94, doi: 10.1145/641205.641211

[18] N. Hajli and X. Lin, "Exploring the security of information sharing on social networking sites: The role of perceived control of information," Journal of Business Ethics, vol. 133(1), Sep. 2014, pp. 111-123, doi: 10.1007/s10551-014-2346-x

[19] D. L. Huang, P. L. P. Rau, and G. Salvendy, "Perception of information security," Behaviour & Information Technology, vol. 29(3), Nov. 2008, pp. 221-232, doi: dx.doi.org/10.1080/01449290701679361

[20] Y. Qu, W. Rong, Y. Ouyang, H. Chen, and Z. Xiong, "Social Aware Mobile Payment Service Popularity Analysis: The Case of WeChat Payment in China," Asia-Pacific Services Computing Conference, Springer Press, Dec. 2015,pp. 289-299, doi: https://doi.org/10.1007/978-3-319-26979-5_22

[21] S. Yang, Y. Lu, S. Gupta, Y. Cao, and R. Zhang, "Mobile payment services adoption across time: An empirical study of the effects of behavioral beliefs, social influences, and personal traits," Computers in Human Behavior, vol. 28(1), Sep. 2011, pp.129-142, doi: 10.1016/j.chb.2011.08.019

[22] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," Computers & Security, vol. 30(4), Dec. 2010, pp. 208-220, doi: 10.1016/j.cose.2010.12.001

[23] Y. E. Lee and I. Benbasat, "Interface design for mobile commerce," Communications of the ACM, vol. 46(12), Dec. 2003, pp. 48-52, doi: 10.1145/953460.953487

[24] M. J. Muller, "Participatory design: the third space in HCI," in Human-Computer Interaction: Development Process, A. Sears and J. A. Jacko, Eds. Boca Raton: CRC Press, pp. 165-180, 2007.

 ISBN: 978-1-61208-616-3