International Journal on Advanced Science Engineering Information Technology

Vol.12 (2022) No. 6
ISSN: 2088-5334

The Impact of Perceived Security and Perceived Trust on the Use of m-Payment Applications in Saudi Arabia

Raed Alotaibi [a], Abdulrahman Alghamdi [b,*]

[a] *Shaqra Community College, Shaqra University, Kingdom of Saudi Arabia*
[b] *College of Computing and Information Technology, Shaqra University, Kingdom of Saudi Arabia*
Corresponding author: [*]alghamdia@su.edu.sa

***Abstract*— A significant technological revolution is currently occurring, with intense competition between companies to deliver their services via emerging technologies. In Saudi Arabia, mobile payment applications have become more important due to the increasing number of users. By filling in the gaps in the Saudi m-payment setting, this work contributes to the theory. It contributes to practice by giving service providers a clear image of the effects Perceived Security and Perceived Trust have on m-payment apps, which is necessary for them to execute their services successfully and effectively. Therefore, this study aims to measure the impact of Perceived Security and Perceived Trust on the use of mobile payment applications. The SEM technique was used to analyze the data. The results revealed that the proposed model is an excellent fit and that the instrument is reliable in the Saudi m-payment context. The SEM results indicated a significant path between (Technical Protection, Transactional Procedures, and Security Statements in m-payment) and (the perceived trust in and perceived security of m-payment applications). It also revealed no significant path between Perceived Security and Trust in m-payment applications. Further, it showed a significant path between (Perceived Security and Perceived Trust) and (the use of the m-payment application). Trust (PT) in m-payment applications will increase the early adoption of these applications. Therefore, the service providers must create and develop secure and trustworthy m-payment applications; otherwise, people will not use them.**

***Keywords*—M-payment; Saudi Arabia; perceived security; perceived trust; technical protection; transaction procedures; security; statement.**

Manuscript received 26 Oct. 2021; revised 10 Mar. 2022; accepted 6 Jun. 2022. Date of publication 31 Dec. 2022.

I. INTRODUCTION

Nowadays, mobile payment applications have become more critical for companies and consumers in trade processes [1], [2]. Payment processes for most bought goods are made using mobile payment applications. According to Al-Marri et al. [3], Saudi Arabia is considered to have the highest growth rate for mobile payments in the Middle East. There were 46.35 million subscribers to mobile telecommunications services by the end of 2020. The growth rate of registered mobile applications in electronic commerce was 460%, and the growth rate of completed orders was 250% in 2020 [4]. In addition, according to Alabdan and Sulphey [5], the use of mobile phones in Saudi Arabia has increased, and the anticipated number of users will be approximately 24 million by 2022. It is further expected that mobile payments in Saudi Arabia will increase progressively because users are becoming dependent on new technologies in trade processes [3]. Therefore, this study aims to measure the impact of perceived security and perceived trust on the use of mobile payment applications in Saudi Arabia.

A. Mobile Payment (m-payment)

Mobile payment (m-payment) is defined as payments using mobile devices, including personal digital assistants, handsets, NFC-based devices, and radiofrequency devices. It is a business movement that includes a mobile device associated with a mobile network to complete financial transactions effectively [6]. The utilization of m-payment systems is progressively successive, and consumers are now accepting it widely [7]. Technology companies, financial institutions, and mobile operators are just part of the venture already considering various advancements and techniques to turn mobile payments into a part of daily life. Dynamism, clients, globalization, and participants will characterize the future scenario of m-payment systems.

The increasing prevalence of m-payment services and the associated technological advances are likely to result in the demise of traditional payment systems. It has been suggested

that with the convenience of diverse m-payment comprising electronic currency, mobile payments, and mediating services, a suitable alternative can be selected for a significant type of transaction [8]. The applicability of mobile payment systems is far-reaching because of the greater development and penetration of mobile devices, by contrast with other structures in the domain of telecommunications.

M-payment strategies are just as reasonable for offline payments as for online payments. Such techniques are desirable for online dealers because of the enormous user base of mobile telephones. Increased utilization of m-payment systems not only lessens a transaction's general charge but also offers superior payment security [9]. Despite this, m-payment systems have experienced difficulties in building a significant consumer base, given security issues and powerlessness to cater to worldwide transactions.

M-payment has played a vital part in transforming conventional payment strategies into advanced payment processes and has prompted modifications in shoppers' practices regarding financial transactions. By contrast, there is a lack of information about the effect of perceived security on the sustainable use of m-payment services, which raises questions regarding its impact on constant use by clients, particularly regarding m-payment services and factors associated with perceived security[10]. Buyers can use it to make offline and online payments from anywhere, and traders can apply it to reduce the cost of transactions and uphold client connections. It is a powerful technology that works with the improvement of a cashless community.

B. Research Model and Hypotheses

The proposed model used in this study (see Fig.1) was adopted in previous studies by Kim et al. [11]. The next section reviews the model's six factors: technical protection, transaction procedures, security statements, perceived security, perceived trust, and using m-payment applications.

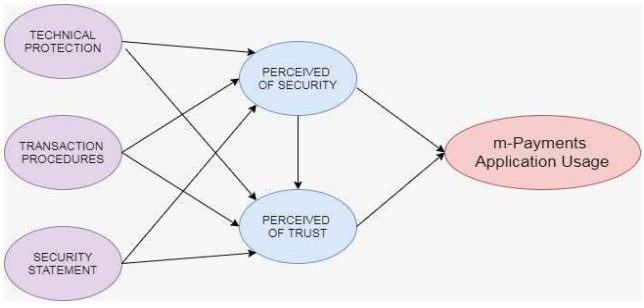

Fig. 1 The proposed model

C. Technical Protection in m-Payment

Technical protection, linked with integrity, privacy, and stability, helps improve clients' apparent security and trust issues [12]. It is argued that in building security and trust in m-payment systems, it is critical to give technical protection to clients [13], [14]. Resistance to and technical reliability of mobile payment systems against security attacks are two elements that affect the security of such systems.

In addition, technical infrastructure, distinct transaction rules, implementation, and lawful elements (for example, legitimate structure) are the significant variables relevant to the security of and trust in m-payment systems [15]. A secure system should have nine components: confidentiality, payment anonymity; authentication, fraud prevention; duplicate spending prevention; transferability; payment privacy; payer traceability; and divisibility. Technical protections (including privacy, stability, and integrity) positively affect perceived trust and security. Adequate technical protection will improve purchasers' perceived security and trust in m-payment systems. The study by Chellappa and Pavlou [16] found that technical protection positively impacted perceived trust and security. Furthermore, previous studies have been found that when m-payment applications are protected, perceived trust and perceived security increase [17], [18]. Therefore, the hypotheses are as follows:

- H1: Technical Protection (TP) impacts Perceived Trust (PT) of m-payment applications.
- H2: Technical Protection (TP) impacts Perceived Security (PS) of m-payment applications.

D. Transactional Procedures in m-Payment

The earliest e-payments empowered clients to carry on transactions electronically by interfacing with financial institutions' sites where they had a bank accounts. It has been suggested that the most developed e-payments have driven not only the mechanization of the approval techniques of transactions [19] but also point to a developmental approach towards the digitization of money, introducing coins that work in the digital domain (for example, advanced digital currencies), among which the most popular model is the so-called 'Bitcoin' system.

Complexity arises from technology and the perspectives of the chain of participants involved in the transaction. This chain encompasses the basic need to guarantee satisfactory security levels, mainly to avoid fraud [20]. These systems can be divided into three major categories: pay online (the client can buy a good or service through the internet); pay in-store (the client can buy a good or service at a mobile terminal and pay electronically at the location of the merchant), and money transfer (the client can buy a good or a service or send money to a third party through an electronic exchange system).

Payments in offline mode do not depend on a third party during the transaction between the purchaser and dealer. It is stated that data exchange happens straightforwardly among the devices belonging to the payer and the payee. From one perspective, this technique avoids the requirement for connecting the payer and payee device with distinct elements, simplifying the management of safety and encryption strategies accordingly. Then again, to pay out the transaction, the payer's telephone contains an electronic wallet that should be loaded in advance [21], [22]. A remote mobile payment (RMP), in which the distance between the terminals is unimportant, might be a transaction made through a mobile device. These kinds of payments depend on the use of an internet program or an SMS. The transaction procedures positively affect the increased level of trust and security for customers when they are using electronic payment systems [8]. Therefore, the hypotheses are as follows:

- H3: Transaction Procedures (TR) impact Perceived Trust (PT) in m-payment applications.
- H4: Transaction Procedures (TR) impact Perceived Security (PS) of m-payment applications.

E. Security Statements in m-Payment

Security statements are the most significant factor affecting buyers' perceived security and trust. The term 'security statement' relates to the information conveyed to the clients (shoppers) for security arrangements and m-payment cycles [15]. Such statements posted on the websites add to the consumer's intention to purchase online. To guarantee the security of the m-payment system, a progression of explicit technical measures is taken and comprises phishing site constant interception, certificate, dynamic password USB key, and NFC technology [13]. Security refers to the transaction safety efforts and collaboration arrangements made by association members of m-payment, for example, specialized organizations and banks for m-payment, to help secure the data and information of the client.

If there are cash losses, trade disputes, or privacy leaks, clients can ensure their genuine interests and rights depend on such associations' security responsibility [23]. It is stated that if clients' perceived risks and protection concerns can be successfully reduced, their apparent security and trust in m-payment can be improved and clients' transactions, privacy and money can be assured. The use of safety procedures, combined with the processing capacity of the devices and ICT networks, permits clients to enable or disable some real-time services. Thus, information protection is guaranteed, allowing access only to authorized parties and only for a period adequate to perform a particular task [19]. Many payment circuits have implemented unique security conventions ready to defend vendors from any transactions considered fraudulent to protect the seller from cancellations. The previous study by Mukherjee and Nath [24] found that security statements in electronic payment systems play a crucial role in impacting users' trust in online payment activities. In addition, the security statements on websites increase consumer purchases [11]. Therefore, the hypotheses are as follows:

- H5: Security Statements (SS) impact Perceived Trust (PT) in m-payment applications.
- H6: Security Statements (SS) impact Perceived Security (PS) of m-payment applications.

F. Perceived Security in m-Payment

Perceived security protection is assumed to be a significant predecessor of trust. It specifies technical safety features in the m-payment application that give the user confidence in the security components during login[25]. The higher the level of security and technical protection, the higher the trust of clients will be. To reduce risks, the exchange of clients' information must be constantly restricted to the time interval needed to complete the monetary transaction [19]. In addition, the clients of m-payment systems may know that throughout the duration of the agreement with the payment service operator, the information stored can be deleted on demand if it is not secure. In m-payment systems, the requirement for security is firmly identified with a potential interception of signals in the radio channel [26]. This requires the utilization of encryption procedures. The versatility of client devices makes the identification and authorization processes in m-payment systems considerably more intricate.

E-payment is different from mobile payment because of the distinctions in the advancements since they made various novel differences on security, for example, risks for mobile devices include theft, damage to the device and misplacement [27]. Perceived Security unequivocally influences customer intention to use m-payment. [28] has stated that consumers did not buy items online since they did not have any certainty of online business. Security and protection concern in m-payment systems affect the attitudes of the consumer. The fear of risk emerges during mechanical transactions because of the absence of human contact. Purchasers worry about payment security because of viruses and hackers and decreases their trust in m-payments that, in turn, can influence their behavior and intention to use the platform. Perceived Security can be designated as transactions at different stages of m-payment that are considered to be safe both financially and with regard to individual information [29]. As it plays a crucial role in clients' practices related to technology, many endeavors have been made to investigate the significant variables of Perceived Security [30]. For instance, by considering cognitive elements, some scientists recognized the intellectual determinants of perceived security, including confidentiality, controllability, non-repudiation, and perceived accessibility. Perceived Security has a crucial role in influencing consumers to use electronic payment activities. Therefore, if the level of security is very low in electronic payment systems, users will not use them [17]. A positive relationship has been found between perceived security in electronic payment systems and perceived trust in electronic payment systems [11]. Therefore, our hypotheses are as follows:

- H7: Perceived security (PS) impacts perceived trust (PT) in m-payment applications.
- H8: Perceived security (PS) impacts m-payment application usage (US).

G. Perceived Trust in m-Payment

Trust is referred to as affection which is reflected in the certainty that all is well and good with the other party. A purchaser may not buy an item online since the conviction of poor safety [27]. Some researchers have argued that trust may have a greater influence on an individual's intention to use a technical device than its ease of use. Consequently, Perceived Security is a factor of Perceived Trust [27]. Perceived Trust is another key element that influences the intention of the customer to use m-payment. In both online and e-tailor advances, the trust factor affects the buyers' convictions concerning the security of shopping online [31]. In the case of mobile payments, trust in the service provider for the m-payment system is the most significant factor. Since individuals primarily focus on the reputation of the brand, notoriety is equivalent to the service providers or trust of the brand.

With new payment systems in communication technologies, clients' trust in service providers plays a significant part in the use of m-payment. Trust in the technology itself is a fundamental factor if clients are to embrace m-payment services [32]. Trust in the actions of these outsiders remains an issue of concern in the transaction process. The appraisals of the danger, advantages and trust for the sake of m-payment can be related to the demographic features of the buyer. The way m-payment is used will be different across genders and age groups. Different factors, for example, level of education and income, may likewise

influence the usage decisions of the consumer. It has been proposed that the uncertainty resulting from perceived risks makes the trust factor substantially more important in the decision-making process for the consumer [33]. While perceived risk has negative implications for the marketing trade, perceived advantages are positive. Perceived advantage strengthens the significance of the transaction since it adds to the buyer's trust, with risk decreasing as perceived advantages increase. If there is no trust between e-commerce actors and clients, this technology will not be used, which prompts a low level of consumer loyalty and reliability [28]. Trust becomes the ideal method to combat vagueness and uncertainty. Trust and happiness become the significant factors in online payment systems that counterbalance negative and uncertain perceptions. Trust is, in this context, the significant factor affecting mobile payment. Customer trust has a crucial role in influencing consumers to use electronic payment systems. Previous studies have found that consumer trust leads to the spread of trust through electronic payment systems [17], [24]. A recent study by Najib and Fahma [1] found that trust was determined by the intention to use digital payment by Small and medium enterprises (SMEs). Therefore, the hypothesis is as follows:

- H9: Perceived Trust (PT) impacts m-payment application usage (US).

II. Materials and Method

This study used a questionnaire to collect data from participants. The type of measurement scale used in the questionnaire was nominal. A random sampling technique was used to select participants. The target participants were Saudi citizens. The questionnaire had three parts. The first had general information for a participant, including study aims and ethical information. Before conducting this study, ethical approval was sought and granted (Ref: Ethics Appl.270502021). The questionnaire was randomly distributed among 1000 Saudi citizens. Two hundred and sixteen questionnaires were completed and returned. A structural equation model was used to analyze data by assessing the hypotheses.

III. Results and Discussion

A. Personal Information

The results in Table I show that most participants were male (male: n=171, 79.2%; female: n=45, 20.8%). The results also revealed that most of the participants were young (18-40 years) (n=187, 86.6%). The remaining participants were older than 40 (old) (n=29, 13.4%).

TABLE I
Personal Information

Information		Number of participants	Percentage of sample
Gender	Male	171	79.2
	Female	45	20.8
	Total	216	100.0
Age	18-40 years (Young)	187	86.6
	More than 40 (old)	29	13.4
	Total	216	100.0

B. Reliability

The value of the Cronbach Alpha reliability test was above 0.70 for all constructs (Table II), which is considered reliable.

TABLE II
Reliability Coefficient Values

Constructs	Number of items	Cronbach Alpha reliability
Technical protections TP	6	0.702
Transaction Procedures TR	6	0.796
Security statements SS	6	0.870
Perceived of Security PS	4	0.852
Perceived of Trust TS	4	0.878
Using m-payment application US	3	0.801
Overall reliability	29	0.910

C. Validity

A correlation test between questionnaire's constructs was made and the results revealed that there are significant correlations between questionnaire's constructs (Table III). The structural equation model was applied to measure the model's fitness and to assess the hypotheses (see Figure2). The results show that the proposed model in this study has excellent fit values in the Saudi m-payment context ($\chi 2$/df (CMIN/df) =2.668, RMSEA= 0.000, AGFI=0.971, GFI=0.996, IFI=1.001, and CFI=1.000). Further, the results in Table III revealed that there were significant paths between Technical Protection (TP) in m-payment and Perceived Trust (PT) and Perceived Security (PS) in m-payment applications. Therefore, H1 and H2 are supported. The results also revealed that there were significant paths between Transactional Procedures (TR) in m-payment and perceived trust (PT) and perceived Security (PS) of m-payment applications. Therefore, H3 and H4 are supported. Significant paths were also found between Security Statements (SS) in m-payment and Perceived Trust (PT) and Perceived Security (PS) of m-payment applications. Therefore, H5 and H6 are supported. The results also indicated that there was a significant path between Perceived Security (PS) and using the m-payment application (US), so H8 is supported. The results revealed a significant path between Perceived Trust (PT) and using the m-payment application (US), so H9 is supported. The results also showed no significant path between Perceived Security (PS) and Perceived Trust (PT) in m-payment applications. Therefore, H7 is rejected.

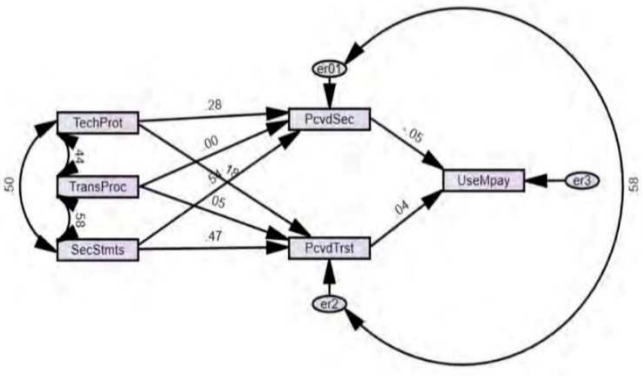

Fig. 2 SEM for proposed model

TABLE III
THE HYPOTHESES' RESULTS

Path	Hypotheses	Hypothesis statement	Path weight Beta β	Overall results
TP→PT	H1	Technical Protection (TP) impacts Perceived Trust (PT) in m-payment applications.	0.178	Significant P<0.001
TP→PS	H2	Technical Protection (TP) impacts the Perceived Security (PS) of m-payment applications.	0.280	Significant P<0.001
TR→PS	H3	Transaction Procedures (TR) impact Perceived Trust (PT) in m-payment applications.	0.001	Significant P<0.001
TR→ PT	H4	Transaction procedures (TR) impact Perceived Security (PS) of m-payment applications.	0.053	Significant P<0.001
SS→PT	H5	Security Statements (SS) impact Perceived Trust (PT) in m-payment applications.	0.471	Significant P<0.001
SS→PS	H6	Security Statements (SS) impact Perceived Security (PS) of m-payment applications.	0.542	Significant P<0.001
PS→ US	H8	Perceived security (PS) impacts m-payment application (US) usage.	-0.047	Significant P<0.001
PT→US	H9	Perceived Trust (PT) impacts m-payment application (US) usage.	0.037	Significant P<0.001

Note: at 95% level of confidence

The SEM results of this study indicate that Technical Protection has an impact on the Perceived Trust (PT) in and Perceived Security (PS) of m-payment applications. Therefore, H1 and H2 are supported. These results are consistent with those of previous studies [11]–[13]. These results were to be expected because Technical Protection is a crucial factor that must exist in m-payment applications because users are focused on specific features before using m-payment, with Technical Protection being the most important. These results indicate that service providers must focus on Technical Protection when they create and develop m-payment applications to increase the users' trust and security in using m-payment applications. In other words, if m-payment applications do not have technical protection, the users will not consider this application trustworthy and secure, leading to them not using it.

The results also revealed that Transactional Procedures impact the Perceived Trust (PT) and Perceived Security (PS) of m-payment applications. Therefore, H3 and H4 are supported. These results are compatible with previous studies, such as [11]. These results were expected because these procedures send messages to users that this application is trustworthy and secure. These results indicate that when the m-payment application fulfills some transactions, the level of user trust and perception of the security of m-payment applications will increase. The service providers must include the Transactional Procedures feature when they create and develop the m-payment applications to increase user trust in and the security of m-payment application use.

Furthermore, the results revealed that Security Statements have an impact on the Perceived Trust (PT) and Perceived Security (PS) of m-payment applications. Therefore, H5 and H6 are supported. These results are consistent with those of other studies [11], [24] and indicate that when the m-payment application has Security Statements such as detailed explanations of how to review, cancel and modify transactions, levels of trust and security will increase. This Security Statements feature should exist in the m-payment application to increase the likelihood of its use.

The results also revealed that Perceived Security (PS) has no impact on Perceived Trust (PT) in m-payment applications. Therefore, H7 is rejected. This result is inconsistent with some previous studies [8]. This result may indicate that when users believe that the m-payment application is secure, their trust in the application/ process is less important. This result may also indicate that some users are confused about the difference between perceived security and perceived trust and may believe that they both refer to the same concept.

In addition, the results revealed that Perceived Security (PS) and Perceived Trust (PT) impact using m-payment applications. So, H8 and H9 are supported. These results are consistent with other studies [17], [34] and indicate that users focus on Perceived Security (PS) and Perceived Trust (PT) when they are using the m-payment application. In other words, a focus on Perceived Security (PS) and Perceived Trust (PT) in m-payment applications will lead to an increase in the early adoption of these applications. Therefore, the service providers must create and develop secure and trustworthy m-payment applications; otherwise, people will not use them.

IV. CONCLUSION

The SEM results showed that the proposed model in this study had an excellent fit with the Saudi m-payment context. In addition, the SEM results revealed a significant path between (Technical Protection, Transactional Procedures, and Security Statements in m-payment) and (Perceived Trust and Perceived Security of m-payment applications). It also revealed that there was no significant path between Perceived Security and Perceived Trust (PT) in m-payment applications. It also showed that there is a significant path between (Perceived Security and Perceived Trust) and (using the m-payment application). This study contributes to the theory by filling in the gaps in the Saudi m-payment context. It contributes to practice by providing a clear picture for service providers about the impact that Perceived Security and Perceived Trust have on m-payment applications if they are to deliver their services successfully and effectively.

REFERENCES

[1] M. Najib and F. Fahma, "Investigating the adoption of digital payment system through an extended technology acceptance model: An insight from the Indonesian small and medium enterprises," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 10, no. 4, pp. 1702–1708, 2020, doi: 10.18517/ijaseit.10.4.11616.

[2] W. Rafdinal and W. Senalasari, "Predicting the adoption of mobile payment applications during the COVID-19 pandemic," *Int. J. Bank Mark.*, 2021.

[3] A. Al-Marri, N. Aldossari, M. Al-Mahish, R. Brizmohun, M. AlKulaib, and A. Alaulami, "Determinants of using the mobile payment to buy coffee among female college students in Saudi Arabia," *Int. J. Adv. Appl. Sci.*, vol. 8, no. 6, pp. 88–93, 2021, doi: 10.21833/ijaas.2021.06.010.

[4] CITC, "Communication and Information Technology Commission Saudi Arabia," 2020.

[5] R. Alabdan and M. M. Sulphey, "Understanding proximity mobile payment acceptance among Saudi individuals: An exploratory study," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 4, pp. 264–270, 2020, doi: 10.14569/ijacsa.2020.0110436.

[6] S.-H. Liao and C.-H. Ho, "Mobile payment and mobile application (app) behavior for online recommendations," *J. Organ. End User Comput.*, vol. 33, no. 6, pp. 1–26, 2021.

[7] I. R. de Luna, F. Liébana-Cabanillas, J. Sánchez-Fernández, and F. Muñoz-Leiva, "Mobile payment is not all the same: The adoption of mobile payment systems depending on the technology applied," *Technol. Forecast. Soc. Change*, vol. 146, pp. 931–944, 2019, doi: 10.1016/j.techfore.2018.09.018.

[8] B. Z, "The Future of the Mobile Payment as Electronic Payment System," *Eur. J. Bus. Manag.*, vol. 8, no. 8, pp. 127–132, 2016.

[9] S. Li *et al.*, "Research on Offline Transaction Model in Mobile Payment System," in *Lecture Notes in Electrical Engineering*, 2019, vol. 542, pp. 1815–1820, doi: 10.1007/978-981-13-3648-5_235.

[10] T. Dahlberg, J. Guo, and J. Ondrus, "A critical review of mobile payment research," *Electron. Commer. Res. Appl.*, vol. 14, no. 5, pp. 265–284, 2015, doi: 10.1016/j.elerap.2015.07.006.

[11] C. Kim, W. Tao, N. Shin, and K. S. Kim, "An empirical study of customers' perceptions of security and trust in e-payment systems," *Electron. Commer. Res. Appl.*, vol. 9, no. 1, pp. 84–95, 2010, doi: 10.1016/j.elerap.2009.04.014.

[12] K. A. A. Sleiman, L. Juanli, H. Lei, R. Liu, Y. Ouyang, and W. Rong, "User trust levels and adoption of mobile payment systems in China: an empirical analysis," *Sage Open*, vol. 11, no. 4, p. 21582440211056600, 2021.

[13] J. Fan, M. Shao, Y. Li, and X. Huang, "Understanding users' attitude toward mobile payment use: A comparative study between China and the USA," *Ind. Manag. Data Syst.*, vol. 118, no. 3, pp. 524–540, 2018, doi: 10.1108/IMDS-06-2017-0268.

[14] J. Zhang and Y. Luximon, "A quantitative diary study of perceptions of security in mobile payment transactions," *Behav. \& Inf. Technol.*, vol. 40, no. 15, pp. 1579–1602, 2021.

[15] E. Oney, G. O. Guven, and W. H. Rizvi, "The determinants of electronic payment systems usage from consumers' perspective," *Econ. Res. Istraz.* , vol. 30, no. 1, pp. 394–415, 2017, doi: 10.1080/1331677X.2017.1305791.

[16] R. K. Chellappa and P. A. Pavlou, "Perceived information security, financial liability and consumer trust in electronic commerce transactions," *Logist. Inf. Manag.*, vol. 15, no. 5/6, pp. 358–368, 2002, doi: 10.1108/09576050210447046.

[17] T. Tsiakis and G. Sthephanides, "The concept of security and trust in electronic payments," *Comput. Secur.*, vol. 24, no. 1, pp. 10–15, 2005, doi: 10.1016/j.cose.2004.11.001.

[18] R. J. Hwang, S. H. Shiau, and D. F. Jan, "A new mobile payment scheme for roaming services," *Electron. Commer. Res. Appl.*, vol. 6, no. 2, pp. 184–191, 2007, doi: 10.1016/j.elerap.2006.07.002.

[19] F. Vatalaro and A. Vizzarri, "M-payment systems and procedures: state-of-the-art and perspectives," *Int. J. Manag. Netw. Econ.*, vol. 3, no. 4, p. 257, 2016, doi: 10.1504/ijmne.2016.079860.

[20] X. Yan, "Towards a More Competitive Mobile Payment Industry: Standardization And Beyond," *J. Compet. Law Econ.*, vol. 17, no. 2, pp. 405–436, 2021, doi: 10.1093/joclec/nhaa029.

[21] Z. Shao, L. Zhang, X. Li, and Y. Guo, "Antecedents of trust and continuance intention in mobile payment platforms: The moderating effect of gender," *Electron. Commer. Res. Appl.*, vol. 33, p. 100823, 2019, doi: 10.1016/j.elerap.2018.100823.

[22] F. A. A. Ramli and M. I. Hamzah, "Mobile payment and e-wallet adoption in emerging economies: A systematic literature review," *J. Emerg. Econ. Islam. Res.*, vol. 9, no. 2, pp. 1–39, 2021.

[23] A. Balapour, H. R. Nikkhah, and R. Sabherwal, "Mobile application security: Role of perceived privacy as the predictor of security perceptions," *Int. J. Inf. Manage.*, vol. 52, p. 102063, 2020, doi: 10.1016/j.ijinfomgt.2019.102063.

[24] A. Mukherjee and P. Nath, "A model of trust in online relationship banking," *Int. J. Bank Mark.*, vol. 21, no. 1, pp. 5–15, 2003, doi: 10.1108/02652320310457767.

[25] L. A. Maureen Nelloh, A. S. Santoso, and M. W. Slamet, "Will users keep using mobile payment? It depends on trust and cognitive perspectives," *Procedia Comput. Sci.*, vol. 161, pp. 1156–1164, 2019, doi: 10.1016/j.procs.2019.11.228.

[26] J. Jiaxin Zhang, Y. Luximon, and Y. Song, "The role of consumers' perceived security, perceived control, interface design features, and conscientiousness in continuous use of mobile payment services," *Sustain.*, vol. 11, no. 23, p. 6843, 2019, doi: 10.3390/su11236843.

[27] W. H. Wong and W. Y. Mo, "A Study of Consumer Intention of Mobile Payment in Hong Kong, Based on Perceived Risk, Perceived Trust, Perceived Security and Technological Acceptance Model," *J. Adv. Manag. Sci.*, vol. 7, no. 2, pp. 33–38, 2019, doi: 10.18178/joams.7.2.33-38.

[28] M. A. Hossain, "Security perception in the adoption of mobile payment and the moderating effect of gender," *PSU Res. Rev.*, vol. 3, no. 3, pp. 179–190, 2019, doi: 10.1108/prr-03-2019-0006.

[29] S. H. Lim, D. J. Kim, Y. Hur, and K. Park, "An Empirical Study of the Impacts of Perceived Security and Knowledge on Continuous Intention to Use Mobile Fintech Payment Services," *Int. J. Hum. Comput. Interact.*, vol. 35, no. 10, pp. 886–898, 2019, doi: 10.1080/10447318.2018.1507132.

[30] F. Liébana-Cabanillas, V. Marinkovic, I. Ramos de Luna, and Z. Kalinic, "Predicting the determinants of mobile payment acceptance: A hybrid SEM-neural network approach," *Technol. Forecast. Soc. Change*, vol. 129, pp. 117–130, 2018, doi: 10.1016/j.techfore.2017.12.015.

[31] L. Gao and K. A. Waechter, "Examining the role of initial trust in user adoption of mobile payment services: an empirical investigation," *Inf. Syst. Front.*, vol. 19, no. 3, pp. 525–548, 2017, doi: 10.1007/s10796-015-9611-0.

[32] J. Park, E. Amendah, Y. Lee, and H. Hyun, "M-payment service: Interplay of perceived risk, benefit, and trust in service adoption," *Hum. Factors Ergon. Manuf.*, vol. 29, no. 1, pp. 31–43, 2019, doi: 10.1002/hfm.20750.

[33] C. Phonthanukitithaworn, C. Sellitto, and M. W. L. Fong, "An investigation of mobile payment (m-payment) services in Thailand," *Asia-Pacific J. Bus. Adm.*, vol. 8, no. 1, pp. 37–54, 2016, doi: 10.1108/APJBA-10-2014-0119.

[34] N. Mallat, "Exploring consumer adoption of mobile payments - A qualitative study," *J. Strateg. Inf. Syst.*, vol. 16, no. 4, pp. 413–432, 2007, doi: 10.1016/j.jsis.2007.08.001.