DOI: https://doi.org
CapitalMark Journal of Marketing & Finance
Journal homepage: https://rjsaonline.org/index.php/CapitalMark

User Trust, Privacy Concerns, and Adoption of Mobile Payment Platforms

Dr. Surayya Jamal[1]
[1]Abdul Wali Khan University, Mardan, 23200, Pakistan
Email: surayyajml@gmail.com

ARTICLE INFO

Received:
May 22, 2025
Revised:
June 17, 2025
Accepted:
July 13, 2025
Available Online:
July 26, 2025

Keywords:
user trust, privacy issue, perceived security, mobile payment adoptions, digital finance, FinTech.

Corresponding Author:
surayyajml@gmail.com

Abstract

Mobile payment platforms have changed the way people process financial transactions through making it possible to make secure, fast and convenient payments digitally. Despite the benefits imparted by technology, there are also large differences in adoption across both types of demographic and geographic segments. This research aims at investigating how trust and privacy of users and security perception can influence the users uptake of mobile payment platforms. A mixed method was used which consisted of the implementation of a quantitative survey (N = 420) and qualitative interviews (n = 20). Findings show that trust has a positive impact on the adoption intention and privacy concern has a negative impact on the willingness to adopt by users. Perceived security plays the role as a mediator between trust and intention to adopt. The findings give insights for designers, developers, financial institutions and policy makers to establish trust in the mobile payments ecosystem by improving users.

Introduction

In the digital world, mobile payment platforms are one of the most disruptive innovations to have hit the financial industry. A mobile payment system is a means by which individuals can conduct financial transactions using their mobile devices such as smart phones and tablets; oftentimes eliminating the physical need for their own cash or even cards. The growth of smartphones and increasing connectivity to the internet as well as the changing digital infrastructures have caused the use of mobile payment technologies to grow across the globe (Dahlberg, Guo, & Ondrus, 2015). Mobile payment solutions take a number of forms, such as mobile wallets (ApplePay, GooglePay), carrier billing, QR code-based, near field communication (NFC) technology, and mobile banking applications that are linked with financial institutions.

Despite high investments in mobile payments by technology companies and financial institutions to encourage the use of mobile payments, the adoption rates have demonstrated strong differences between countries, as well as among demographic groups. Advanced economies have high rates of penetration whereas the rates of adoption are low in many developing countries (Slade, Williams, & Dwivedi, 2015). These differences are attributed not only to economic but also psychological, social and technological perceptions that influence user's behavior.

Among the most important factors affecting the rate of adoption of mobile payment would be trust, privacy, and perceived security on the part of the user. As applied here to mobile payments, trust is the extent to which users have confidence in it - to get the job done - at times without exposing themselves to undue risk. It includes trust in technology, service providers as well as regulatory frameworks underlying mobile payment ecosystems. Trust is especially important for mobile payments because transactions are connected with sensitive financial information and are not managed physically, which might make users feel they are at a greater risk (Gefen, Karahanna, & Straub, 2003).

Privacy concerns are one other major obstacle to adoption. Mobile payment systems often require the users to provide them with personal and financial information, including bank accounts, phone numbers, and identification information. Many users fear that they cannot be protected from third-party access to such data, its abuse, or sharing without their consent. High profile data breaches and cyberattacks contribute to all these fears and lead to skepticisms in the safety of mobile payment platforms (Malhotra, Kim, & Agarwal, 2004).

Perceived security is how users evaluate their confidence of the security of a mobile payment platform in ensuring the security of their data and financial assets from unauthorized access, fraud and cyber threats. Security concerns are common, especially among users who are not terribly technologically savvy but do not know the encryption and authentication protocol used by mobile payment systems. Visible security measures such as biometric authentication, multi-factor authentication and encrypted data transmission can help to build confidence in users and minimize the risks (Kim, Shin, & Lee, 2010).

The balancing act between the trust, privacy, and perceived security is important in explaining the adoption behavior of mobile payment users. The theoretical underpinning of this study is based on some of the established models i.e. Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT) and Protection Motivation Theory (PMT). Traditional TAM focuses on what are the most commonly used determinants of technology adoption which are perceived usefulness and ease of use (Davis, 1989). However, when we talk about mobile payments, with its associated financial risk and personal information, constructs such as trust and privacy, become just as, if not more, significant. The UTAUT framework has social influence and facilitating conditions added to the model to account for mobile payments that are associated with unique psychological factors that require expanded constructs that are in addition to the original framework of the model (Venkatesh et al., 2003). Protection Motivation Theory is an account that assumes that users balance the threat with their perception of their ability to deal with that threat and their sense of security of the features and institutional protections (Rogers, 1975). These theoretical perspectives are applied as an entirety to read the adoption of mobile payments in this research.

In practice the adoption of mobile payment platforms have been applied to a variety of applications from e-commerce (e.g. purchasing in shops and venues), or payment of bills, peer-to-peer payments, to financial service - financial applications (e.g. loan, investment products). The introduction of the Covid-19 pandemic made the rise of digital payments even bigger as consumers were seeking contactless alternatives to making cash payments. Nonetheless, there is the presence of trust and privacy issues that ensures adoption is not just a matter of necessity and also of confidence and risk reduced.

This study aims to fill in a number of gaps in the extant literature. While there has been a lot of research work on individual factors like perceived usefulness and ease of use, there are few instances that have considered trust, privacy concerns and perceived security general, in a combined model of adoption. Additionally, many studies have examined developed economies with robust cybersecurity frameworks which has left little knowledge on the nature of situations where regulatory protections may be less robust. By taking a mixed methods approach, an integrated understanding of the interaction of these psychological and technological factors of user adoption of mobile payment platforms is sought by this research.

Literature Review

Research into the adoption of mobiles payments demonstrates a wide variety of user behavior influenced by, amongst other factors, technological, socioeconomic, and psychological factors. According to Dahlberg et al. (2015), the adoption of mobile payments depends on how people experience the usefulness and convenience of mobile payment technology in consideration with problems that are related to the risk and uncertainty. In advanced markets such as China, mobile wallets have been widely welcomed because of integrated ecosystems which combine social media, e-commerce and financial services (Lu, Yang, & Wang, 2011). The opposite is true for areas that tend to be lower in trust and have less structure around their laws and both of these tend to report more gradual adoption.

Trust in Mobile Payments

Trust is one of the most researched factors related to adoption. Defined in terms of willingness of placing trust in service provider in the face of threat trust plays a crucial role of reducing uncertainty in mobile transaction (Gefen et al., 2003). Trust has different dimensions, such as trust in technology (known as system trust), trust in organizations (called institutional trust) and trust in laws and safeguards (known as regulatory trust). It has always been concluded from studies that the higher the trust level was, the increased the adoption intention (Slade et al., 2015; Oliveira et al., 2016).

Privacy Issues of the Digital Financial Services

Privacy issues when users perceive the use of the personal information as their right to collect, access or share it without consent. Malhotra and colleagues (2004) conceptualizes privacy concerns as an important barrier in e-commerce and the framework has been adapted in the context of mobile payments. Users are often afraid of the usage of their data, the data tracking to know their spending habits, and their financial data being accessed without their permission. Xu, Teo and Tan (2011) find that increased concern for privacy has a direct effect on reducing trust in digital platforms and, in turn, adoption intention.

Security Perceptions and Risk For Fraud

Security perception can be defined as users judgment about security and reliability of mobile payment platforms Security concerns may include concerns of identity theft, fraud and unauthorized transactions. Various visible security features such as encryption, biometric authentication and fraud alerts enable network users to associate increased security and trust (Kim et al., 2010). Studies show that there is positive correlation between perceived security and adoption intention (Shin, 2010) in which security mediate the relationship between trust and adoption behaviour.

Perceived Risk Framework

Featherman and Pavlou (2003) describe perceived risk as multiple-dimensional, which includes financial risk, performance risk, privacy risk and psychological risk. "In the case mobile payments, financial and privacy risks become very well marked, given the presence of money transactions and personal information in direct". Higher perceived risk generally lowers the adoption intention suggesting the need to address such perceived concerns through technological and policy interventions.

Extended Adoption Models

While the traditional models, like TAM and UTA, have contributed to valuable groundwork for studies, there are suggested extensions by scholars to include trust and risk constructs in order to improve financial technology adoption explanations. Wtracho, Zhou, Zhou, & Zhou, Z. (2011) TAM as a construct: Integrating trust and perceived security boosted the prediction of mobile payment adoption. Oliveira et al. (2016) also illustrates the importance of combining risk perceptions and trust on extended UTAUT models for FinTech applications.

Trust-Privacy Interplay

Studies mention that trust and privacy issues are inter-related constructs. High privacy concerns can lead to reduced trust which can result in low adoption intention (Xu et al. 2011). On the contrary, if the users have the perception that a platform takes data protection seriously, then privacy issues have faded away and the degree of adoption is likely to increase. This two way relationship implies that trust does not only directly influence adoption, but also the way privacy issues influence decision making.

Regionalization and Cultural Influences

Cultural and regulatory condition visually moderate the consequence of trust and privacy on to adoption. Schwartz (2004) says that societies where laws protecting the data exist are linked with high levels of trust in digital systems whereas countries where the regulatory environment is lax have high levels of skepticism. Hence, it is necessary to understand the psychological constructs and the environmental factors to comprehend the behavior of adoption.

Research Gaps

Despite a lot of research on the adoption of mobile payment, there are gaps. Few, if any, studies, however, have analyzed, simultaneously, trust, privacy, and perceived security in one empirical context. Moreover, the majority of empirical studies are conducted in developed economies, which limits the generalizability of this study to emerging markets in which digital trust might be moderated by other socioeconomic variables. This study helps to contribute to the literature as it integrates all of these variables and presenting the use of a mixed-phase method for the nature of capturing both the quantitative pattern and the quality of the information.

Methodology

This study uses mixed-method research design, which combines quantitative and qualitative research methods so as to provide the study with a holistic view, in order to understand the influence of trust, privacy issues and perceived security to mobile payment adoption. A hybrid approach of both qualitative and quantitative methods allows checking for quantitative validation of the relations and better descriptions of the user experiences for deeper insights on the relation of trust on mobile payment intentions in user payments. To know the effect privacy issue has on adoption. To examine the potential moderating effect of perceived security and trust on the adoption intention.

Population and Sampling

The target population comprised of the mobile payment users between the ages of 18 and his 90s years living in the urban areas of various socio-economic backgrounds. Stratified random sampling method was used by which different gender, age groups and education levels are represented. A total of 420 responses of the survey were collected and 20 semi-structured interviews were conducted for a qualitative insight.

Measurement Instruments

Components of a questionnaire used for survey were validated constructs based on the existing research:

- User Trust: According to Gefen et al. (2003).
- Privacy concerns Can be from Malhotra et al. (2004).
- Perceived Security: Based on Kim et al. 2010.
- Adoption Intention (from Venkatesh et al (2003).
- Answers were given using a 5 point Likert scale ranging from 1 (Strongly disagree) to 5 (Strongly agree).

Reliability and Validity

Cronbach's alpha coefficients for all constructs were > 0.82 for all constructs indicating high levels of internal consistency. Confirmatory factor analysis (CFA) was conducted in order to establish the convergent and discriminant validity.

Data Collection Procedure

The data collection was done during six weeks. Surveys were posted on social media websites, emailed, and distributed to users of FinTech forums. The semi-structured interviews took the form of phone and voice call and were digitally recorded and transcribed.

Data Analysis and Discussion

Quantitative data were conducted through the help of the statistical packages such as statistical package services (SPSS) and AMOS:Descriptive statistics were used in order to understand the characteristics of the sampleCorrelation analysis was used to test the relationships that occurred between variablesRegression analysis was used to measure the strength and direction of the effectsStructural Equation Modeling (SEM) was used to examine the overall modelQualitative data were analyzed using thematic analysis, and the general patterns as well as user perceptions were identified.

Descriptive Statistics

Of the people who were surveyed, 57% were male and 43% were female. Users said they have experience using sites such as EasyPaisa, JazzCash, paypal and google pay.

Table 1. Descriptive Statistic

Variable	Mean	Standard Deviation
Trust	4.15	0.72
Privacy Concerns	3.52	0.87

Perceived Security	3.95	0.75
Adoption Intention	4.08	0.69

Correlation Analysis

There was a positive association between trust and adintention ($r = 0.63$, $p < .001$). Privacy concerns was found to be negatively correlated with adoption intention (r=-0.40, p=.00). There was a positive relationship between perceived security and trust ($r = 0.58$, $p < .001$).

Regression Analysis

Table 2. Regression Results

Predictor	Beta Coefficient	p-value
Trust →Adoption Intention	0.51	< .001
Privacy Concerns →Adoption Intention	−0.29	< .01
Security →Trust	0.43	< .001

Qualitative Themes

Interview analysis revealed three recurring themes:

- Transparency Builds Trust: A number of users indicated that they have trust for the platforms who were communicating on privacy policies and security measures.
- Fear of Use of Data in an Abusory Manner: Privacy concerns were about sharing of data without an authorized use and fears associated with theft of identity.
- Security Features Boost Confidence: Users named multi-factor authentication, encryption and biometric sign-in as top confidence benefits.

Interpretation of Findings

The quantitative results confirm the idea that trust is the biggest predictor of adoption intention. Privacy issues are a key aspect in terms of user's willingness to adopt mobile payments, whereas perceived security builds trust. The qualitative findings complement such results, because users stressed the importance of transparent policies and robust security features.

Discussion

This research contributes to the understanding of the key role of trust in the acceptance of mobile payment platforms. Users are more inclined to adopt systems that they feel are trustworthy, reliable and secure. Trust plays a psychological buffering role: it makes the global uncertainties of the digital financial transactions less uncertain. Unlike traditional banking is face to face, mobile payment is remote interaction with complex technologies. Perceived risk is negated through trust and engagement is invited.

Privacy issues arose as major impediments for the adoption. Users showed fear of having their personal and financial data accessed without their consent, of having it sold to third parties or used for purposes unrelated to their original intentions, such as marketing. Such perceptions deter the use of trust and bring down adoption intention. Previous studies have indeed shown that privacy considerations have a negative influence on user behavior in digital systems (Xu et al., 2011).

Perceived security represents a direct and indirect influencer in the adoption. Directly, people who are confident with security mechanisms are more comfortable with mobile payments. Indirectly, perceived security promotes trust which results in a higher intention to adopt. Visible security features like biometric authentication, encryption and fraud detection tools help in building this perception of safety.The balance between trust, privacy and security implies that adoption decisions are multidimensional. The problem, however, is that looking for factors like ease of use is not sufficient if privacy and security are not taken into account. Mobile payment providers therefore must take an approach that combines trust, privacy concerns and security measures. Regulatory frameworks and consumer education also play an important role in generating user perceptions and trust.

Conclusion

This research focused on the determination of the importance of user trust, privacy issues and perceived security as influencing factors to the adoption of mobile payment platforms. The results showed that trust is the most important predictor for adoption intention and privacy concerns have a negative effect on the willingness to adopt. For example, perceived security increases trust, which indirectly leads to adoption.These outcomes highlight the importance of establishing trust through transparent policies, and effective security implementation and credibility from institutions. Mobile payment platforms should be good communicators themselves-obtaining specific information on how user data is stored, used, and protected. Security mechanisms such as encryption, multi-factor authentication, and biometric verification should also be standard features.Policymakers and regulators also should have a role to play and enforce data protection laws, establish security standards, and ensure compliance. Consumer education campaigns can complement and increase understanding and dispel endearing fears.

To summarize the findings, tackling the issues of trust, privacy, and security together can play an important role in increasing adoption of mobile payments to drive financial inclusion and engage various population segments collaboratively privacy concerns combine to pose a significant obstacle to adoption The study also confirms that privacy concerns act as a significant hurdle to adoption. Users often view mobile payment platforms as places to store sensitive financial and personal information such as banking information, transaction records, and personal ID. Concerns about such issues as unauthorized access to their data, disclosure to third parties or potential for identity theft decrease acceptance of these services. This would also be in line with findings by Malhotra, Kim, and Agarwal (2004) who argued that privacy concerns in the digital environments can have a substantial effect on user confidence. Moreover, the qualitative analysis suggests that the privacy threat perceived by users is not solely shaped by the technology being used, but is affected post-its broader socio-cultural aspects, e.g. media reports of cyberattacks, anecdotal accounts of fraud and a general distrust of financial institutions.

Perceived security becomes a direct and indirect factor for adoption. Security features such as multi-factor authentication, encryption, biometric verification, and transaction alerts are a direct reassurance of the safety of their digital transactions. Indirectly, these features attract trusts by signaling the commitment of the platform to protect the data of its users. Users trust the credibility and professionalism of platforms with a robust security infrastructure and feel confident while adopting it, which in turn facilitates adoption. Notably, in the study, perceived security is more influential for users with their prior experiences of mobile payment fraud or security breaches, indicating an effect of experience on sensitivity to security cues.

The interplay between trust, privacy and what is seen as security implies a dynamic multidimensional scheme to understand adoption behaviour. While trust has a positive effect on adoption, privacy concerns have a counterbalancing negative effect, and perceived solutions to privacy issues mitigate the negative effects of privacy concerns, while the latter reinforces trust. This finding is in favor of an integrated approach with respect to mobile payment design which should focus not only on the technical level of reliability, but also on the level of transparent communication and policy. Providers should actively educate users about privacy protections, the intention of data gathering and security measures to curb some of the fears and strengthen trust.

Recommendations

- Strengthen security of encryption and authentication protocols
- Provide clear and easy-to-understand privacy policies
- Organize awareness campaign on security of Mobile Payments
- Perform data protection regulations and compliance audits
- Perform regular system updates to counter threats that have emerged
- Encourage third party security audits
- Provide fraud assurance and reimbursement policies
- Improve customer support to financial dispute resolution
- Design intuitive and trusting and trustworthy user interfaces

References

1. Dahlberg, T., Guo, J., & Ondrus, J. (2015). A critical review of mobile payment research.
2. Slade, E., Williams, M., & Dwivedi, Y. (2015). Mobile payment adoption: A literature review.
3. Gefen, D., Karahanna, E., & Straub, D. (2003). Trust and TAM in online commerce.
4. Li, X., & Yeh, Y. (2010). Security issues in mobile payments.
5. Xu, H., Teo, H., & Tan, B. (2011). Privacy concerns in mobile commerce.
6. Davis, F. (1989). Perceived usefulness and ease of use in TAM.
7. Venkatesh, V. et al. (2003). UTAUT model.
8. Malhotra, N., Kim, S., & Agarwal, J. (2004). Internet users' information privacy concerns.
9. Shin, D. (2010). User adoption and mobile payment security.
10. Kim, G., Shin, B., & Lee, H. (2010). Security and trust in mobile payments.
11. Featherman, M., & Pavlou, P. (2003). Perceived risk in e-services.
12. Zhou, T. (2011). Extended TAM for mobile payments.
13. Oliveira, T., et al. (2016). Trust and risk in mobile payment adoption.
14. Taddicken, M. (2014). Privacy and trust online.
15. Liébana-Cabanillas, F., et al. (2020). Mobile payment risk perceptions.
16. Rogers, R. (1975). Protection Motivation Theory.
17. Donner, J., & Tellez, C. (2008). Mobile banking for development.
18. Alalwan, A. (2018). Mobile banking acceptance frameworks.
19. Chawla, D., & Joshi, H. (2019). Attitudes toward mobile wallets.
20. McKnight, D., & Chervany, N. (2002). Trust constructs in IT.
21. Pavlou, P. (2003). Consumer trust in electronic commerce.
22. Lu, Y., Yang, S., & Wang, Y. (2011). Mobile payment adoption in China.
23. De Luna, I., et al. (2016). Mobile payment intention determinants.
24. Khalilzadeh, J., et al. (2017). Biometric authentication in mobile payments.
25. Lee, K., & Chung, N. (2009). Risk and trust in electronic payment systems.