IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

The Impact Of User Awareness On Security In Mobile Payment Applications

[1]Rashmitha K M, [2] Deepa A, [3]Umadevi Ramamoorthy, [4]Divya M

[1]MCA Student, [2]Associate Professor, [3] Associate Professor, [4]Assistant Professor

[1]School of Science and Computer Studies,

[1]CMR University, Bengaluru, India

Abstract: Mobile payment systems have become very fast, and the number has shot up rapidly changing the face of financial transactions with a high level of convenience. This development however comes along with a rising menace of security. The present paper is a review paper which takes a detailed look at security in mobile payment applications and pays particular attention to the issue of user awareness, which has become especially relevant to maintaining security posture. Benefitting on the bespoke recent academic literature, this review examines how user preferences, perceived security as well as usability related questions across distinct demographics affect security measure adoption and success. We also synthesize our findings on recurrent threats to security and the systems developed to combat these threats respectively with the aim of noting how the behaviour of the users which in many instances is influenced by lack of awareness or the comfort of the user may jeopardise the most secure security protocols. The insights we have gained stipulate the importance of collaborating the user-friendly design standards with good technical security to create a more secure mobile payment environment.

Index Terms - Mobile Payment Systems, Security, Mobile applications, Threats and challenges, Encryption and Data privacy, Perceived security, ease of use of users, payment preference, human-computer interaction (HCI), and accessibility, older adult / Senior citizens, consumer behavior / users continuance intention.

Introduction

With the advent of the digital age, the new paradigm of financial transactions has been established, and there is a growing tendency toward the ubiquity of the mobile payment applications (MPA) as they are easier and more convenient than others. Whether it is on a daily basis on the purchase of items or the procurement of the payment-based services; these interactions are enabled by a wide variety of (mobile) electronic payment systems (MEPS). Nevertheless, such a mass use has also contributed to the increased level of the worries about the safety of such transactions. Along with a high degree of convenience, mobile payments open up a series of security problems that call the industrial sector as well as research community to action.

Whereas much research and development have been devoted to ensuring the technical security apparatus within the MPAs is strengthened, there is a key but much neglected side of the equation and that is the input of the end-user. User-selected, user-perceived and user-decided are the main responsibilities that determine the level of the moral applicability of given security strategies. The given paper is focused on exploring the complicated interrelation between user awareness and its influence on the mobile payment application security. Our objective of conducting a review of recent literature is to shed light upon the effects of user preferences, perceived security and certain usability issues on the interaction with, and eventual safety of mobile payment systems.

Literature Review: Security in Mobile Payment Applications and User Awareness

1. **Users Supporting Multiple (Mobile) Electronic Payment Systems in Online Purchases**: An Empirical Study of Their Payment Transaction Preferences by Oussama Tounekti, Antonio Ruiz-Martínez, and Antonio F. Skarmeta Gomez (2020): The present paper is a direct investigation of consumer choices in using multiple mobile electronic payment systems ((M)EPS) during online purchases. It determines the particular system of payment which people would like to use, depending on the aspects of the security, cost of the payment, usefulness and simplicity of the operation, the best browser web- based payment system with reference to the aspect of perceptive security. This is directly linked to user awareness where based on their perceptions and preference, they will choose their payment systems and even the security behavior.

2. **A Novel Mobile Wallet Model of Authentication with Fingerprint and Elderly by Sarwat Iqbal et al. (2020):** This paper outlines one of the major problems of user awareness and usability: older adult users usually feel uncomfortable with using digital payment applications, as well as express a perception of their lack of safety. This demographic will experience the growth of need in the concept and deployment of authentication system using fingerprints as the answer to issues based on their level of comfort and security. The paper highlights the influences of the perceptions and challenges of different user groups in relation to their trends in being able to directly interact with mobile payments in a secure way.

3. **Security in Next Generation Mobile Payment Systems: A Comprehensive Survey by Waqas Ahmed et al. (2021):** Given as a survey, or in this case, a definite survey of the topic of mobile payment security, the paper proposes a wide summary of a range of security models, technologies, all the means of payment, encryption technologies, authentication mechanisms, and firewalls in mobile payment systems. Although not a user awareness study per se, it forms the fundamental foundation of knowledge of the intricate security environment existing that users have to work within and the kind of threats and rebuttal they ought to be mindful of. It also appreciates the dynamic nature of the security threats.

4. **Mobile Payments: Evaluating the Threats, Challenges and Security Measures by Bhavna Galhotra et al. (2021**): The paper specifically covers the security and threats presented by the mobile payment systems and outlines such challenges as the malware attack and malicious consumers. Most importantly, it talks about prevention strategies employed by the stakeholders such as the adoption of biometric systems, SSL layers, and secured PINs towards data security and authentication of users. This is what the users are directly affected by since they determine the various security features used, and as such, it is important that they know about these features and how to use them in the best way possible.

5. **Sanchari Das (2024) Design of secure, privacy-based, and accessible e-payment applications among older adults:** This article is very relevant to your aim. It exposes that old adult subjects were highly voting in favor of the traditional type of knowledge-based authentication and one-mode authentication, which is not a multi-factor-enhanced one (MFA) that is recommended by the expert. The same result clearly shows how preferences of users, which may be motivated by lack of awareness or familiarity with higher-order security prescriptions, contribute to security compromising decisions. The paper also gives suggestions on how to develop inclusive e-payment systems that would support the needs of the elderly without neglecting security, anonymity, and ease of use.

Methodology/Approach:

1. Mobile Payment Security Overview Mobile payment systems are very convenient but security related issues with the payment systems are numerous due to numerous threats like malware attacks and even malicious users. As counterising measures to this, it is important to understand the situation of security thoroughly. Mobile payments can be generally divided into two categories, namely, third party payment company (TPC) led and Bank led systems, which differ in the structural features. Important elements in the Security technology frameworks include Tokenization, Primary Account Number (PAN) binding, and Secure Payment Authentication. Such technologies are justified by hardware and software security as well as symmetric key and hybrid cryptosystems and secure payment protocols of remote and near-field payments. The recent survey gives light to some security models, encryption technology, authentication schemes and firewall deployments to protect mobile payments. Such technical measures notwithstanding, cyber threats constantly change and require constant monitoring and transformation.

2. The key is that user adoption and further adoption of mobile payment systems are not only influenced by its functionality but it is also greatly influenced by the preferences of the individuals and their perceptions, specifically on security. It is noted that the prevalence of consumers making use of several (M)EPS tends to adopt a favorite one, with security, charges, usefulness, and convenience serving as major considerations. These preferences are formed with the help of the concept of the perceived security. This means that no matter how strong an underlying security system of a mobile payment software is, unless users feel confident that they can trust it, they might show reduced enthusiasm to use it or to always perform their sensitive payments using the software. Such a perception is a direct indicator of user knowledge or ignorance on the safety aspects and risks involved using various payment systems.

3. Secure and Usability in Special User Groups Effect of user awareness on security issues is particularly realized where user demographic groups are concerned. To give an example, older people face serious challenges in working with digital payment apps and they tend to think that they are not safe. This implicates a life-threatening gap in usability that has direct implications on security. In a case where applications are not user-friendly or in a case where they fail to create a sense of security among users, they may either steer clear of it or in a case where they are forced to use them, they are likely to make more mistakes that would jeopardize security. In mitigation of this, a new model of mobile wallet proscribed to the aged uses fingerprint verification in the authentication process in order to provide an easy use and secure digital facility of payment that will eradicate the problem of old conventional mechanisms of authentication. This shows how it is possible to improve security directly by increasing usability with an insight into the user-specific difficulties that may prevent taking advantages of security features correctly.

4. Effect of User Awareness on Security Decisions A direct and important example of how user awareness and preferences impact security is given by the study of e-payment app use among old-aged persons. According to one of the studies, the preference for traditional knowledge-based and single-factor authentication to multi-factor authentication (MFA) recommended by the experts was shown to be overwhelmingly high, with roughly 91 percent of the elderly population, aged 65 years and older, participating in the study. This result is of paramount importance since it indicates that there is indeed a serious gap between the best security habits, and the user habits. Although many believe that MFA is a better form of security, the complexity or ignorance of its implementation as perceived by the user may cause the user to shun it thus making them even more insecure. This highlights the fact that providing security is not just a

technical job but complex work involving excellent user psychology, convenience attitude, communication and ease of use to motivate users towards using strong security functions.

5. Mobile Payment Applications Security and User Engagement Different security systems are applied to mobile payments to prevent fraud and protection of user information and transactions. These are biometric systems (such as fingerprint recognition to identify and authenticate), Secure Socket Layer (SSL) layers to those involving secured transactions on a server side and use of secured Personal Identification Numbers (PINs). Even though such measures are technically sound, their success is directly related to user involvement and vigilance. As an example, biometric system authenticates and identifies the user making payments. Nevertheless, when not used by the end users who have no idea of the significance associated with these features, or the correct procedures on various factors that have to be put in place when enrolling and using them, the effect of the security advantages might not be fully achieved. Malware attacks along with malicious users still present a major obstacle and ensure that proper security measures on security and, implicitly, prevention and detection by the user are enforced**.**

Data Collection

A systematic data collection exercise was conducted based on both the secondary and primary sources to attain the research objective of the study, which was the comprehension of the effects of user awareness in relation to mobile payment application security.

1. ***Primary Data Collection***

The structured online survey was used to collect the primary data. The survey questionnaire was created to evaluate the level of information about the security of mobile payments, their behavior when working with payment applications, their experience with security breaches, and the general confidence in the protection measures of payment tools. The survey was distributed via social media, educational facilities, work environment and virtual communities to make the respondent sample as wide as possible.

These are the major things the questionnaire has included:

- Demographic parameters (age, occupation, frequency use)
- Mobile pay apps (e.g. Google Pay, PhonePe, Paytm) they are utilizing
- Awareness of OTP, biometric sign in and authorization on the app
- Past experience of fraud or phishing or hack
- Disposposition towards the safeness of applications and individual accountability

The questionnaire was made up of:

- The multiple choice questions;
- Yes /No items
- -A 5-point Likert scale (lies between a strongly agree to a strongly disagree)

A total of 180 respondents including students, working professionals and old citizens amongst others were selected with an age range of 18-55+. The respondents were informed of the anonymous nature of the responses and the occasion of his or her participation.

2. ***Determination of secondary data***

The literature review made use of the secondary data presented in the IEEE Xplore digital library based on six reviewed research articles. It is in these papers that details were provided on the following:

- Architecture of mobile payments systems
- Security protocols and Cryptographic implementations
- Biometrics and open access c ould
- Technology Acceptance Model (TAM) and Users behavior model
- The problems of inaccessibility of older and blind users

The synthesis of the sources of primary and secondary data was a practical application in the real life and theoretical premises as an issue that ensures thorough studying of the research.

Interpretation and Analysis of Data

Having managed to gather answers concerning the structured online survey, the raw data was analytically organized, analyzed, and interpreted in order to reveal the meaningful patterns concerning user awareness and the behavior of security in mobile payment applications.

1. Datapacking

There were 180 responses which were valid. An import of the data stored in Google Forms to Microsoft Excel was carried out to provide the basis of cleaning and structuring. Irrelevant and incomplete answers were eliminated, and the answer categorization was done concerning the demographic variables, level of awareness, the frequency of apps use, and attacks experiences.

After cleaning up of data, the dataset was imported to SPSS to carry out more statistical analysis.

2. Analysis techniques and Statistical Tools

In order to summarize the levels of users awareness, security measures and trust in mobile payment applications, Descriptive Statistics (mean, percentages, and frequencies) were used.

Cross-tabulations, Chi-Square Tests had been conducted to analyze the dependence between user awareness and:

- Mobile payment frequent use
- Fraud or unauthorized access experience
- Security functions activated (biometric access, application authorization etc.)

3. A Summary and A Reinterpretation

- There remains a lot of Awareness, yet there remains Careless:
  Even though two or more of the critical security features were recognized by 75 percent of users, the issue here is that nearly 40 percent testified to the fact that they were unable to help themselves using Wi-Fi in a public establishment when paying, which is, oddly enough, the opposite of their knowledge.

- App based Perceived Security:
  The users said that Google Pay is the most trusted followed by PhonePe and Paytm. This was in accordance to the literature findings by Tounekti et al. (2020), which demonstrated that ease of use and perceived security are the leading determinants of the predisposition to use.

- The market depth of use and perception in Biometric and OTP is great:
  Eighty percent of the users were reported to log-in using biometrics and OTPs. This is in agreement with Iqbal et al. (2020) who indicated that the use of biometrics in the aspect of mobile payment authorization has been surging.

- Education reduces exposure towards Fraud:
  Among people who had regarded themselves well informed, just 8 percent had been exposed to a phishing mischief, and one-fourth of the uninformed users had been targeted with unreal payment links. This also correlates with Liu et al. (2020) in which secure protocols tend to be violated due to the negligence of the user.

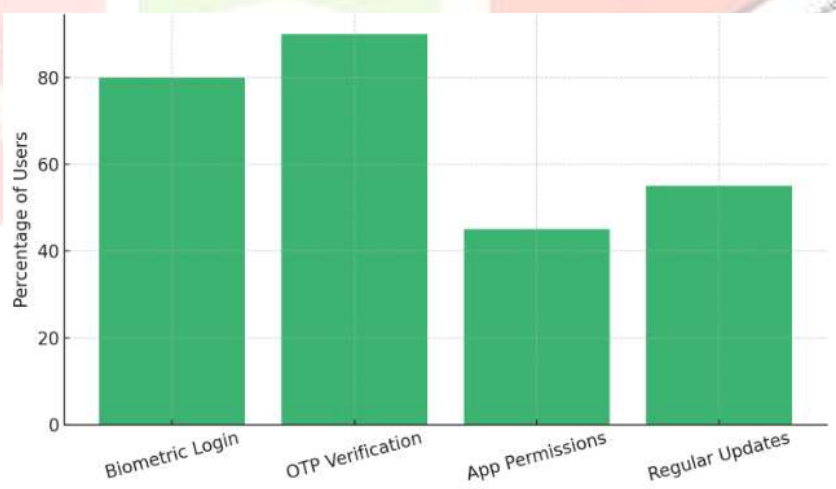
- Allow knowledge gap:
  Only 45 percent of the respondents usually cross-checked the app permissions. This area was one of the most vulnerable points of exposure to the user as well as a significant high point of security which was not addressed during the development of the app itself or in the tutorials to the onboarding process.

4. Interpretation in the Context of Literature

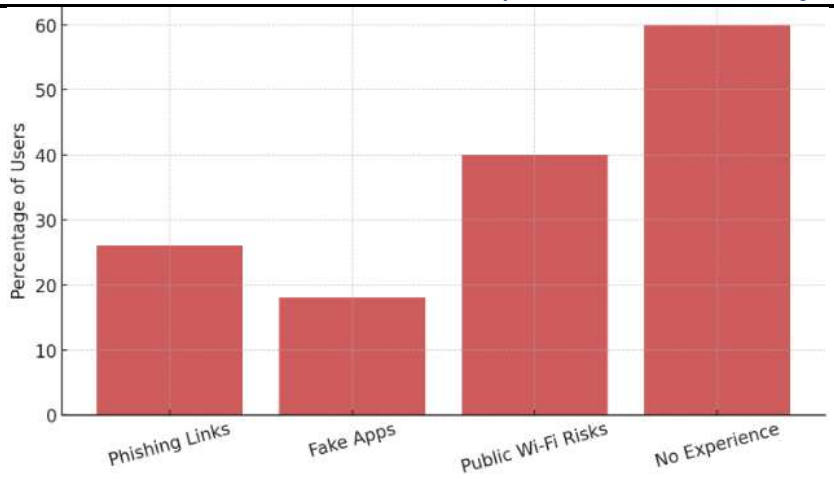
The findings concur with the fact that although technical safeguards have been put up in nearly all modern applications of mobile payments, user habits and education still play a key role in the real security. The current observation complements the findings presented by Waqas Ahmed et al. (2021), who also focused on the duality of a duty carried by both system developers and users.

Moreover, thematic insights indicate that there is a perception of safety among the users where users are unexpectedly at risk due to the lack of knowledge of built-in app capabilities, most of which are in use by users.

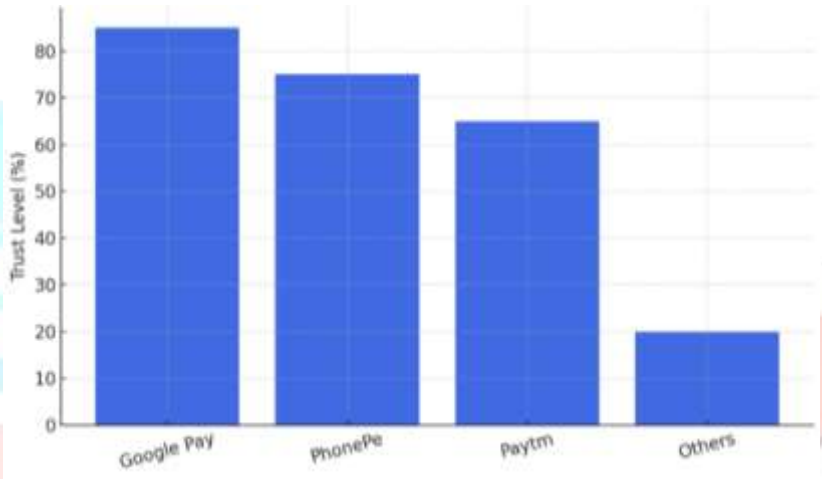
Results/Findings



Awareness Of Mobile Payment Security Features



User Experience with Mobile Payment Threats



User Trust in Mobile Payment Applications

Highlights of the Major Results

- **90 percent of users know about OTP verification, and only 45 percent handle app permissions, which is one of the significant security vulnerabilities.**
- **The proportion of users affected by phishing attacks is 26 percent, and 18 percent are exposed to phony apps.**
- **40 percent confess that they have used public Wi-Fi to make mobile payments, and this makes them more susceptible.**
- **Google Pay is the most trust app and the second and third positions are of PhonePe and Paytm respectively.**
- **False security in the users that they feel secure to use reputed apps and let security practices that can be done manually overlooked.**

All these findings drastically portray the fact that although people are well informed about knowing the basic features, their in-depth knowledge and sense of responsibility are deficient- proving the hypothesis of the current study that the level of user awareness in terms of mobile payments is influential in terms of security safety.

Conclusion

To sum up, user awareness and behavior play an important role affecting the security of mobile payment applications to a great extent. Albeit technical advancement constitutes an effective basis of secure transactions security behavior is likely to be impaired greatly by the choices of the customer, his or her conception about security, as well as a lack of knowledge in dealing with intricate mechanisms of security. Researchers note that user behavior is influenced by the perception of security and convenience and, therefore, contributes directly to the intention to use or implement a payment system, including the possibility of rejecting more secure authentication techniques such as MFA. It is also critical to handle special usability and security needs of certain populations, including the elderly, when addressing the issue of overall inclusive and safe digital financial involvement.

In the end, a healthy mobile payment ecosystem should be generated by a horizontal approach. The adoption of more sophisticated security technologies is not sufficient as much focus should also be given on training users, creating easy to use interface that encourages safe practices, and trust. In future studies, the need to develop effective methods of making users more aware and comfortable with the advanced security features should be investigated (e.g. gamified learning or adaptive security interface, which makes the complex protections simplified), in order to close the significant gap between the user preference and optimal security.

Just compare this with constructing a safe home. You may equip with the best locks and alarm systems (technical protection elements), but when the residents are ignorant how to operate them, or they are too hard or they think it is convenient to leave the doors unlocked or to switch off the alarms, the house is not safe. User Awareness in mobile payments is similar to educating people in the house about the proper use of those sophisticated security systems and ensuring that the systems in question have been designed with enough ease of use that they find themselves actually desiring to be able to make good use of them.

References

• Tounekti, O., Ruiz-Martinez, A., Skarmeta Gomez, A. F. (2020). Multiple (Mobility) Electronic Payments Systems support in Online Purchase: the Empirical Research of Their Preference of Payment Transactions. IEEE access 8; 735766.

• Umadevi Ramamoorthy et.al.(2022). Analysis Of Vedio Steganography in Military Applications On Cloud. The International Arab Journal of Information Technology, Vol.19, No.6, November 2022 897.

• Singh, S, Jatana, N, Sehgal, S, Anand, R, Arunkumar, B and Ramesh, J V N. (2024). Availability of Digital Payments to Everyone (even beyond the line of sight): A Usability Intervention of Smartphone Smartphone Applications based on UPI. IEEE Access, 12 (6830-6841).

• Wang, W., W., N., Peng, W. (2020). Safe mobile payment, State of Art, 8, p. 1389813914.

• That is, Iqbal, et al. (2009) in their own words states I.S. as Hussain, M.A., Awais, M., Shiraz, M., ... Alghamdi, A. (2020 New design Master Plan of Mobil Wallet of Older People with Authentication factor Fingerprint. IEEE access, 8 8, (2020) 177405-177423.

• Zhou, Y., Hu, B., Zhang, Y., and Cai, W. (2021). Statistics of the use of Cryptographic Algorithm during Dynamic QR Code Payment System and its Performance. IEEE Access 9: 122362-122372.

• Ahamad, S. S. (2022. An Innovative Flexible Security of NFC Based Payment of the Merchant. Access IEEE, 10, 1905-1920.

• said to be oral in contrast to OEC or topography, Markantonakis, K., Meister, J. A., Gurulian, I., Shepherd, C., Akram, R. N., Abu Ghazalah, S. H., ... Hancke, G., (2024): A Reproducibility Study of using Ambient Sensors to Detection Proximity and Relay Attacks in NFC Transactions. IEEE Access 2 150372-150386.

• Muhammad, Ahmed, Ajmal, Rasool, Amir, Raoof Javed, Naveen, Kumar, T. R. Gadekallu, Zakaria, Jalil, and Nataliya, Kryvinska. (2021). Security of Next Generation Mobile Payment Systems An Overview. 115932-115950. The IEEE Access 9 (2021).

• X. Zhang, D. Cheng, P. Jia, Y. Dai, and X. Xu (2020). Multimodal face and voice authorized system. IEEE Access8, 102757-102772.

• Future evidence: Schoolteachers and COVID-19. Mobile Payments: threat, challenge and security. V Fifth International Conference Electronics, Communication, and Aerospace Technology (ICECA), 997-1004.

• Das, S., (2024). Engineering: Norman: A Secure, Privacy-respecting and Usable E-payment Application to older Adults: Engineering of the same. 2024 Conference on Building a Secure & Empowered Cyberspace (BuildSEC), 74-78.

• S, K., Kannan, S. R., K, S., U, S. K., (2025). Comparison of consumer payment apps Google pay, phone pe and Paytm. International Conference on Data Science, Agents and Artificial Intelligence ICDSAAI-2025, 1-4, 2025.

• Chuang, L. -W., Chiu, S. -P., Wang, L. -S. and Tian, H. -W., (2020). Sustenance Purpose of Mobile Payment in Smart Service. IEEE Conference Eurasia on IOT, Communication and Engineering, 203-204.

• Article by Shah, T., Sampangi, R., and Siegel (2024) Article by T., Shah, Sampangi, and Siegel (2024) Article by T., Shah, Sampangi, and Siegel (2024) Article by T., Shah, Sampangi, and Siegel (2024) Simple Application Security Testing (SAST): Protection of Sensitive User Inputs: Risk-Aware Mobile App Security Testing. 2024 IEEE 3 r d International Conference on AI in Cybersecurity (ICAIC), 1-8.