International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Addressing the Trust Factor in Mobile Payments through Enhanced Security Controls

Hemant kumar P. Bulsara, Esha A. Pandya

Abstract: ***Trust plays a key role in the acceptance of a new payment system and is at the heart of any method of payment. Companies have been using mobile payments for over a decade. Because of the high uncertainty and security issues accompanying mobile payment, developing trust of users is critical to enable their adoption and use. Customers will use mobile payments as long as they have trust in this relatively new mode of payment together with dependence on its services and applications. In this context, recent studies indicate that trust in mobile payment systems (MPS) is not uniform among users despite the fast development of mobile technology and the new modes of payment. The aim of this paper is to provide a number of suggestions to assist developing greater trust in the mobile networks and provide customers with a secure and befitting experience that will influence mobile payment adoption in turn.***

Index Terms: Mobile Payment, Trust, Security issues, Mobile Payment Adoption

I. INTRODUCTION

Society at large is now relying less on physical mode of payment i.e. cash and majority of the businesses these days accept debit and credit cards. The payment scenario has evolved from cash to cheque system, from cards to online payment and recently to mobile payments. Businesses which were reluctant to accept cards a few years back have now embraced the change in order to speed up the payment process and retain or grow their clientele. Customers these days can easily pay their monthly bills, taxes or rent using a credit. A recent research indicated that by 2025, 75% of all transactions will happen cashless. The growing popularity of mobile banking and mobile payment apps indicate consumers' willingness to adopt smart devices for their financial transactions [13].

With new suppliers, new platforms, and new payment instruments launching on a near-daily basis, payments are now propagating rapidly. As the behavior of customers change, Omni Commerce's expectation arises – that's the capacity to pay with the same technique whether purchasing in-store, online, or via a mobile phone. This change shows that distributors need to adapt to mobile payments that are quick, easy and safe. Mobile payments can be defined as paying for the purchase of goods and services using a mobile device at a point of sales terminal of a retail outlet or over the Internet.

Manuscript published on 30 September 2019
Dr.Hemantkumar P. Bulsara, Applied Mathematics & Humanities Department, S.V.National Institute of Technology, Surat, India. Email: hemantbulsara@gmail.com
Ms. Esha A. Pandya,S.R.Luthra Institute of Management, Surat, India. Email: eshapdy@gmail.com

Payment can be made via SMS, app, mobile browser, quick response (QR) code or near field communication technology (NFC). Simultaneously, the growth of peer-to-peer payments, one-touch checkout options and the evolution of sharing economies have led to new opportunities for remote mobile payments [13].The rise of mobile payments

- Smartphone penetration and market share of mobile operating system are the key indicators of budding mobile payment acceptance. Smart phones have made it possible for consumers to connect to different channels, which make it easier for the consumers to use mobile phones for making payments. Other important enabler of mobile payment acceptance is the rise of mobile commerce.
- Stakeholders from different sectors, comprising card networks, financial institutions and traders have shown larger interest in the evolving mobile payment sector – by introducing proprietary alternatives or allowing third-party players. Stakeholders are trying to adjust as soon as the technological advancements take place. Financial services industry start-ups, incumbents and technology suppliers are developing fresh services that help shape customer preferences.
- Mobile transactions can quicken the checkout process, which benefits both customers and merchants, in comparison to chip-and-signature cards. In case of mobile payments, the mobile device is a substitute for a card. A user can enter debit or credit card details in a mobile app in advance and use it to make payments anywhere or a user can operate a mobile payment app in a store and let the cashier scan it for payment or a user can opt for tap & pay via NFC payments. Mobile payments merely provide a variety of ways to execute transactions at various places.

Mobile payments are gaining momentum, but still account for a tiny proportion of total consumer payments. The major hurdles for consumer adoption are safety and privacy issues. Consumers are concerned of disclosing their financial details and consider it a risky affair. They often come across the news about privacy breaches and thefts of sensitive data due to which they are not much confident that evolving technology can maintain their cash secure. It is critical that the present mobile payment systems solve this problem and gain consumer confidence with appropriate safety checks and simple use cases from the outset [14].

II. LITERATURE REVIEW

Different studies have focused on the influence of trust on user adoption of new payment methods across the past decades. Several researchers focused their research on the influence of trust on the adoption of new payment systems by consumers, including mobile payment systems.

In the domain of mobile services, trust can be defined as an extent to which a user believes or have confidence in specific service that is considered to have no safety and privacy threats [1]. In other way, trust means relying on to mobile services now with the hope that they will be risk-free, and in the future you will receive intangible benefits in some ways at an indefinite time. Cultivating the trust of customers is a time-consuming method for mobile service providers. Trust is difficult to attain, but easy to lose. Trust is a basic component, according to several researches, that affects the desire of customers to use the MPS [2]-[5]. As reported by numerous m-commerce studies, there is not enough trust in mobile payment systems and wireless transactions [6]-[10]. One reason is that financial details and bank balances may alter during m-payment operations before a consumer can understand it; an issue that impacts the trust of the consumer in these transactions [11].

M-payments face issues such as likely security loopholes through wireless networks and technological constraints on mobile devices to perform a complete transaction (authentication of customers, authorization of merchants and banks, and transfer of funds). Security control is regarded to be an important antecedent of trust and a significant factor for m-commerce and e-commerce's continuing growth and future. In particular, it is hard to build trust in mobile payments because of security issues [12]. It can therefore be inferred that lack of trust is deemed a significant obstacle in the initiation of customer interactions, which, despite its potential, has a negative impact on m-payment acceptance and growth, and that it is essential to establish adequate security controls.

III. METHODOLOGY

To gain insight into consumers ' minds; how they approach safety; the data and related information was collected via personal interview method from the mobile payment users. The data was collected from a total of 1087 respondents from four major cities of Gujarat – Ahmedabad, Vadodara, Surat and Rajkot during February - March, 2019. Secondary data has been collected through various journals, websites and reports.

IV. RESULTS

Mentioned below are the results of the personal interviews, which indicate the direction businesses may consider when they want to develop mobile payment systems of their own.

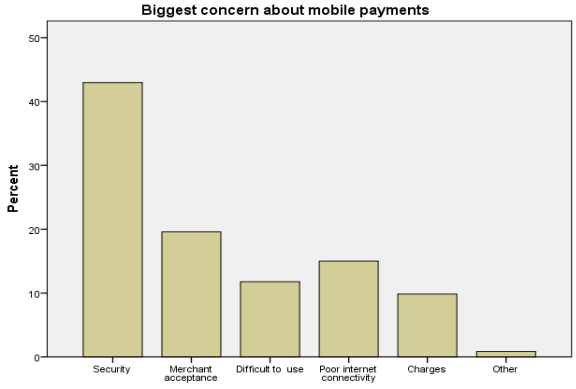


Fig. 1. Opinion about biggest concern in mobile payments

From the above chart, it can be observed that "Security" is the biggest concern of users while using mobile payments.

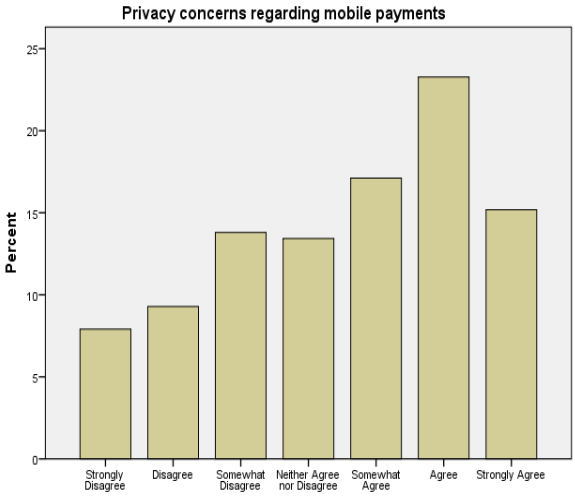


Fig. 2. Opinion about privacy concerns in mobile payments

The above chart indicates that a majority of the users are having privacy concerns while using mobile payments.

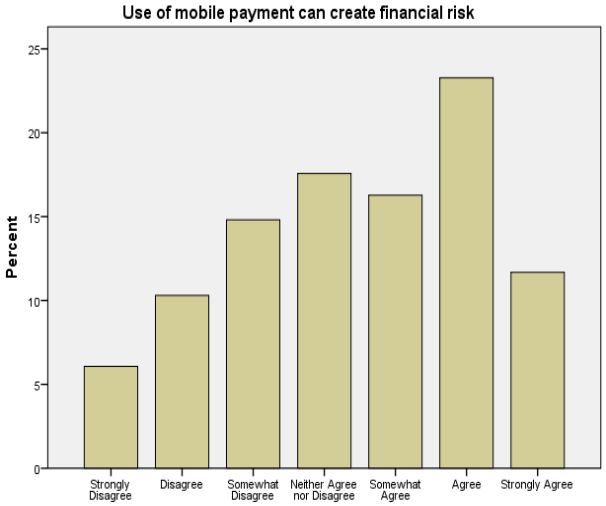


Fig. 3. Opinion about mobile payments creating financial risk

From the above chart, it can be observed that majority of the users believe that using mobile payments can cause financial risks.

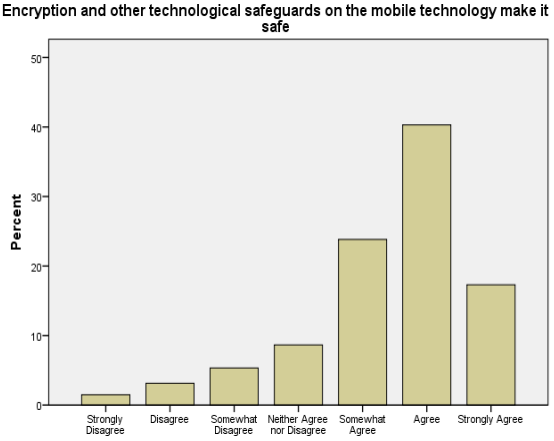


Fig. 4. Confidence on various technological safeguards

It is evident from the above chart that majority of the users have confidence that encryption and other technological safeguards can make mobile payment systems secure.

The above results indicate that businesses and mobile payment developers should focus on building systems which can address security and privacy concerns. The way to resolve the same is to use advanced security measures which can generate trust in the minds of users.

V. DISCUSSION

For those organizations who have developed or are planning to release a mobile payment system, there are a series of steps they can take to create confidence with their customers. In an environment where there are numerous third parts apps which are not well regulated, m-payment applications should be designed in a way so that they can survive safely and can take suitable actions to protect themselves.

In order to execute various stages of security, a security oriented approach is very important. Due to this, the users also feel protected. This can include using tools like biometric verification which includes iris, facial and fingerprint scanning to visual icons indicating proper working of the system.

App developers need to assess their audience and the intent of their application. For certain cases, it might be suitable to link a customer's account with a social network, however in majority cases like financial or public services, the customers are quite vigilant regarding sharing of personal details hence it should be dealt with utmost care. The comfort of the user requires to be part of the design, from registration to daily use of the app. Additionally, it is required that a uniform experience is delivered irrespective of the type of device and system software.

Biometric authentication can improve user comfort, lead to confidence and acceptance of new services. Consumers have started embracing biometric authentication. Face recognition and iris scanners have also begun to rollout alongside fingerprint readers. A remarkable illustration of the same can be found in the launch of Selfie Pay by MasterCard or iris scanning feature of high end Samsung mobiles. Developers ought to find ways about how to integrate all these facets which are reverberating with the end users.

The subsequent user acceptance can then be taken as a positive feedback [15].

A. Security Solutions for additional and customizable security

To design defensive apps

Application developers require executing a comprehensive security framework that can handle ever changing malware. Some alternatives like purpose-made software development kits (SDKs) can tackle the issue by means of security measures that enable applications to:

- Protect own self by using coding procedures along with cryptography
- Identify risks via secure environment detection
- Respond threats arise: give alert to a dedicated server for risk management while simultaneously withholding the processing

Well built authentication

Software development kits (SDKs) let app developers to design strong user authentication techniques.

Biometric technology is mostly well-known among end-users and is a mobile-friendly innovation. Majority of people are confident about their face and fingerprint being sufficiently distinct to serve as their key for authentication In addition, if app developers wish to investigate other alternatives for strong authentication, they may think about using a one-time password or Out- of-Band (OOB) authentication via Push notification, being a technique in which a push alert is delivered to the customer's mobile, asking permission regarding any of the app login. Protected PIN entry systems also deserve attention because they are incorporated in the app rather than availing the handsets ' standard PIN keypad. This ensures protection of delicate authentication features like personal identification numbers (PIN) and passwords. Furthermore, SDKs allow digital signatures to be designed and it comes across to be one more remarkable illustration of a robust authentication technique to secure important transactions. Nevertheless, in spite of executing sound authentication, maintaining a dynamic customer experience is very importance while taking into account above mentioned authentication alternatives [15].

Table I: Summary of different techniques of protection.

Examples of threats in device	Mobile security solutions
Revealing susceptible data like passcodes, revealing private information of customers (details regarding name, contact number, email id etc.)	**Encryption** and **strong authentication** for securing admission to personal data
Unauthorized use of user interface (UI): Using keylogger malwares to collect Passwords or PINs in order to let a hacker log into a customer's bank account. Additionally, a hacker can also log into remote information systems of an organization and take away sensitive information.	**Using backup virtual keypads** incorporated into the design of the app rather than using an integrated keyboard. **Biometric authentication such as fingerprint scanning** Above remedies can deliver robust client authentication
Theft of mobile devices and password by unlawful parties. They can break in to the bank accounts of the clients or can access online government accounts of a client and take away critical business information	To use a risk management software that can identify abnormal conducts and implement security measures consequently **Managing mobile device:** in this case users can delete the device memory even being far off and can maintain privacy of their data
Modified transaction values: for example, how much cash consumers want to move via m-Banking	Continuous transaction monitoring (CTM) Intrusion detection system (IDS) Security incident and event management applications (SIEM)

B. Adopting a layered approach to security

Layered Security

It is important to implement a layered approach towards security in order to cope up increasing complexity from the end of hackers. It is not sufficient to depend on a single protection technique; extra security layers need to be in place based on the risk involved. It can be for overall use and also for the initial enrollment.

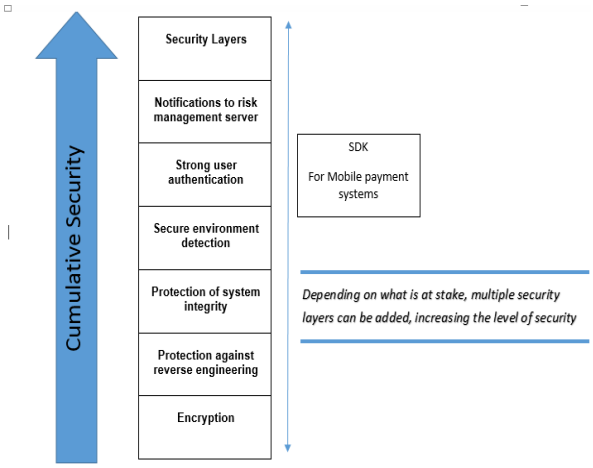
Technically, numerous security layers can be joined together to enhance the security standard at large. Hackers are apt in recognizing loopholes in mobile networks; Security layers can be used to protect various parts of apps so that it becomes difficult for the hackers to attack. This layered approach can be facilitated by SDKs.

This methodology can be facilitated by SDKs so it is suggested to use them to defend against cyber attackers.

Fig 5. Mobile payment software security, a layered approach

Risk Management

A vital aspect of layered security approach is risk management. Security systems can soon become outdated as cyber threats are not stagnant but continually growing and becoming even more unpredictable. Due to the dynamic nature of threats, an adaptive risk management system is



required, so that it can withstand different conditions and execute accommodative safety measures when the apps are being used for specified purpose. These type of systems can sense unusual transaction forms, evaluate the threats associated with the transaction, stop the transaction remotely, and request customers to authenticate additionally for mitigating the threats. Critically, this assessment is carried out during execution itself so as to ward off risks without delay [15].

VI. CONCLUSION

Given that our dependence on mobile is increasing, it is essential that we can trust the devices and services we use each day. This is why mobile security solutions are designed to support various security frameworks that include both software and hardware, to offer the state-of-the-art digital security and promote the implementation of services in a fragmented mobile industry.

Protection is essential in every step of the user journey. Robust authentication and securing identity are needed to guarantee appropriate security for mobile software.

In addition, to trigger service acceptance, it is essential to include user comfort and the ' mindset of security ' as part of the designing security. In specific, it is becoming more common to use biometry such as iris or facial identification and fingerprint readers. Clearly, consumers value strong protection to the extent that many are ready to pay a premium for guaranteed safety.

At a stage where cyber threats are constantly increasing and users have access through their smart phones to an exceptional amount of precious services, it is vital that each player is equipped. It would be risky to handle cyber security as an afterthought; efficient risk management and assessment systems need to be available to safeguard end users, otherwise confidence in mobile payments will be significantly undermined and the complete potential of mobile technology will not be attained. The chance is out there as consumers would adopt digital identity if they knew their mobile phones were 100% secure. By working together, key stakeholders such as governments, banks, mobile network operators and IT specialists can create a safe environment that mitigates the ever-growing landscape of cyber security threats, making mobile payment systems more confident.

REFERENCES

1. S. Gao, J. Krogstie and PA. Gransæther, "Mobile Services Acceptance Model", in *International Conference on Convergence and Hybrid Information Technology*, 2008.
2. T. Nguyen, T. Cao, P. Dang and H. Nguyen, "Predicting Consumer Intention to Use Mobile Payment Services: Empirical Evidence from Vietnam", *International Journal of Marketing Studies*, vol. 8, no. 1, pp. 117-124, 2016. Available: 10.5539/ijms.v8n1p117.
3. X. Gong, K. Zhang, S. Zhao and M. Lee, "The effects of Cognitive and Emotional Trust on Mobile Payment Adoption: a Trust Transfer Perspective", in *the Pacific Asia Conference on Information Systems*, Chiayi, Taiwan, 2016.
4. H. Xin, A. Techatassanasoontorn and F. Tan, "Exploring the influence of trust on mobile payment adoption", in *Pacific Asia Conference on Information Systems*, 2013, pp. 1-17.
5. A.Duane, P. O'Reilly and P. Andreev, "Realising M-Payments: modelling consumers' willingness to M-pay using Smart Phones", Behaviour& Information Technology, vol. 33, no. 4, pp. 318-334, 2012. Available: 10.1080/0144929x.2012.745608.
6. B.Corbitt, T. Thanasankit and H. Yi, "Trust and e-commerce: a study of consumer perceptions", Electronic Commerce Research and Applications, vol. 2, no. 3, pp. 203-215, 2003. Available: 10.1016/s1567-4223(03)00024-3.
7. C.Kim, M. Mirusmonov and I. Lee, "An empirical examination of factors influencing the intention to use mobile payment", Computers in Human Behavior, vol. 26, no. 3, pp. 310-322, 2010. Available: 10.1016/j.chb.2009.10.013.
8. K. Lee, H. Lee and S. Kim, "Factors influencing the adoption behavior of mobile banking: A South Korean perspective", *Journal of Internet Banking & Commerce*, vol. 12, no. 2, p. 1, 2007.
9. Y. Li and Y. Yeh, "Increasing trust in mobile commerce through design aesthetics", *Computers in Human Behavior*, vol. 26, no. 4, pp. 673-684, 2010. Available: 10.1016/j.chb.2010.01.004.
10. Park and Y. Sujin, "The moderating role of consumer trust and experience: value driven usage of mobile technology", *International Journal of Mobile Marketing*, vol. 1, no. 2, pp. 24-37, 2006.
11. Wu and S. Wang, "What drives mobile commerce?",*Information & Management*, vol. 42, no. 5, pp. 719-729, 2005. Available: 10.1016/j.im.2004.07.001.
12. Y. Shao Yeh and Y. Li, "Building trust in m-commerce: contributions from quality and satisfaction", *Online Information Review*, vol. 33, no. 6, pp. 1066-1086, 2009. Available: 10.1108/14684520911011016.
13. "MEDICI | Overview of the Payments Industry", *MEDICI*, 2019. [Online]. Available: https://gomedici.com/overview-of-the-payments-industry. [Accessed: 10- Aug- 2019].
14. C.Insights, "Barriers to use of Mobile Payments | WEX Inc.", WEX Inc., 2019. [Online]. Available: https://www.wexinc.com/insights/blog/inside-wex/barriers-to-use-of-mobile-payments/. [Accessed: 12- Aug- 2019].
15. Gemalto, "Building trust in mobile Apps: The consumer perspective", 2019.

AUTHORS PROFILE

Dr. Hemant kumar P. Bulsara, is an Associate Professor (Management) and Head- Applied Mathematics & Humanities department of S. V. National Institute of Technology (NIT), Surat, India. He holds over 20 years of experience. His interest areas include Technology Innovations and Entrepreneurship, Technology Business Incubation, Marketing Management, Supply Chain Management and General Management. He has been guiding Ph.D. scholars in these areas. He holds around 75 research papers to his credit. Dr. Bulsara is an editorial board member and reviewer of several international and national Journals of repute.

He is regularly been appointed as a keynote speaker, conference chair and a session chair at National and International level. He has visited many countries like USA, UK, France, Netherlands, Finland, Italy, Bali Indonesia, Hong Kong, Macau, Thailand, Malaysia, Singapore etc.

Ms. Esha A. Pandya received her Bachelor of Engineering (Computer Science) degree from Gujarat University, Ahmedabad, India and Masters of Business Administration degree from Veer Narmad South Gujarat University, Surat, India. She is a PhD scholar (Management) at S.V.National Institute of Technology, Surat and also working as an Asst. Professor (Management) at S.R.Luthra Institute of Management, Surat. She has over 10 years of experience. Her areas of interest include M-commerce, Consumer Behaviour, Banking & Financial Services and Management Information Systems.