MOBILE BANKING IN INDIA: ISSUES AND CHALLENGES

LAABH SINGH
Assistant Professor
Department of Commerce
Govt. P.G. College, Jind

ABSTRACT

Mobile banking is a service provided by a bank or other financial institution that allows its customers to conduct financial transactions remotely using a mobile device such as a smart phone or tablet. Unlike the related internet banking it uses software, usually called an app, provided by the financial institution for the purpose. Mobile phone is a common technology device that became part of every individual in the information era. Mobile Banking is an emerging alternate channel for providing banking services. India is the second largest telecom market in the world, which is having high potential for expanding banking services using mobile. However, mobile banking has not become the choice of millions of people. This study also defines the role of mobile banking in payment industry by providing ease to existing bank customers and by offering new services to the customers in emerging areas. By using mobile banking technology users has been much quicker than the adoption of online banking more than a decade ago. This research paper defines many issues and challenges which are facing in use of mobile banking.

Key Words: Mobile Banking, Issues, Security & Challenges, Banking & Financial Services

INTRODUCTION

The earliest mobile banking services used SMS, a service known as SMS banking. With the introduction of smart phones with WAP support enabling the use of the mobile web in 1999, the first European banks started to offer mobile banking on this platform to their customers.

Mobile banking before 2010 was most often performed via SMS or the mobile web. Apple's initial success with iPhone and the rapid growth of phones based on Google's Android (operating system) have led to increasing use of special mobile apps, downloaded to the mobile device. With that said advancements in web technologies such as HTML5, CSS3 and JavaScript have seen more banks launching mobile web based services to complement native applications. These applications are consisted of a web application module in JSP such as J2EE and functions of another module J2ME.

A recent study (May 2012) by Mapa Research suggests that over a third of banks have mobile device detection upon visiting the banks' main website. A number of things can happen on mobile detection such as redirecting to an app store, redirection to a mobile banking specific website or providing a menu of mobile banking options for the user to choose from.

Mobile banking is a system that allows customers of a financial institution to conduct a number of financial transactions through a mobile device such as a mobile phone or personal digital assistant. Mobile Banking refers to provision and an ailment of banking- and financial services with the help of mobile telecommunication devices.

Mobile banking can be said to consist of three inter-related concepts:

- Mobile accounting
- Mobile brokerage
- Mobile financial information services

Most services in the categories designated accounting and brokerage are transaction-based. The non-transaction-based services of an informational nature are however essential for conducting transactions - for instance, balance inquiries might be needed before committing a money remittance. The accounting and brokerage services are therefore offered invariably in combination with information services. Information services, on the other hand, may be offered as an independent module.

Typical mobile banking services may include:

Account information

1. Mini-statements and checking of account history
2. Alerts on account activity or passing of set thresholds
3. Monitoring of term deposits
4. Access to loan statements
5. Access to card statements
6. Mutual funds / equity statements
7. Insurance policy management

Transaction

1. Funds transfers between the customer's linked accounts
2. Paying third parties, including bill payments and third party fund transfers(see, e.g., FAST)
3. Check Remote Deposit

Investments

1. Portfolio management services
2. Real-time stock

Support

1. Status of requests for credit, including mortgage approval, and insurance coverage
2. Check (cheque) book and card requests
3. Exchange of data messages and email, including complaint submission and tracking

4. ATM Location

Content services

1. General information such as weather updates, news
2. Loyalty-related offers
3. Location-based services

A report by the US Federal Reserve (March 2012) found that 21 percent of mobile phone owners had used mobile banking in the past 12 months.[7] Based on a survey conducted by Forrester, mobile banking will be attractive mainly to the younger, more "tech-savvy" customer segment. A third of mobile phone users say that they may consider performing some kind of financial transaction through their mobile phone. But most of the users are interested in performing basic transactions such as querying for account balance and making bill.

LITERATURE REVIEW

Heggade O.D.(2000) analyzes the range of customer services provided by the banks by the side of with their impact on customer-banker relations. This Study shows with Indian banks in general and banks of Dakshana Kenara District in exacting. The study also make known that banking routine of people in this district are good and better so that customers are satisfied with banks' customer services.

Mishra J.K. and Jain M. (2007), this research defines the several dimensions of customer satisfaction in private sector and nationalized banks. This research concludes that satisfaction of the customers is a very useful quality for the present organizations, on condition that without comparison reasonable edge which helps in creating and developing a long term relationship in addition to trademark impartiality.

Uppal R.K. and Kaur R. (2007) this analyze the effectiveness of all bank groups in the post banking sector improvement time. The research recommends some evaluates for the improvement of good organization of Indian nationalized banks.

Zafar M.K., Qureshi T.M. and Khan M.B. (2008) this research analyzes the customer acceptance of online banking. This research concludes that widely held of customers are compliant online banking for the reason that of many favourable issues, security, usefulness and confidentiality are the main look at factors to acknowledge online banking system in Pakistan.

Sawhney S., Kamble S. S., Bansal R. (2009) this research defines online service quality factors that make possible the client's fulfilment for the e-travel and e-mart online retail. Additionally they assess how these measurements are perceived by the customers for offering an objective determines of service performance.

Bahl, Sarita (2012) this study defines that privacy and security factors are the big issue in mobile banking. According to this study if security and privacy factors or issues are recognized then forthcoming mobile banking system would be great successful.

V. Devadevan (2013) this research defines the Issues and Challenges of mobile banking in India. This Research explores the opportunity of technology make possible services to provide better customer experience and convenience. India is the second largest telecom market in the world, which analyze the security issues in Mobile banking among the banking customers in India.

Manav Aggarwal (2014) this research analysis that the importance of mobile banking is largest financial institutions which on a regular basis discover the chance of technology to offer enhanced customer service utilities. This research analyzes that the customers to carry out a number of financial transactions by using mobile devices.

OBJECTIVES OF THE STUDY

The main objective of the present study is to understand the issues and challenges involved in using m-banking as a business tool and to give recommendations for the solution of security issues.

CHALLENGES OF MOBILE BANKING

There are some issues and challenges that need to be addressed, which includes technical, regulatory and legal issues. A few important challenges are addressed:

A. **Economic Challenges:** The rural population in India is spread across 600,000 villages, each with a low transaction value. Profitability can only be achieved by large volumes, requiring significant initiative from financial institutions. Unlike the very successful M-PESA of South Africa, whose model has been very successful due to the lack of alternative payments in South Africa, India does possess some infrastructure in the forms of postal payments, reasonable transport and local governments (Brown, et.al., 2003). Therefore, any mobile banking must be inexpensive enough to be attractive for the end-customer over existing methods.

B. **Regulatory Challenges:** Although the RBI is supportive of mobile banking in India, there are many regulations that are being put into place:

   a) **Restricted to Financial Institutions:** The guidelines state that only existing financial institutions and banks are allowed to offer mobile banking. Although the guidelines cover Microfinance Institutions (MFIs), significant economies of scale cannot be achieved by these due to existing large fixed costs. For a very inexpensive solution, it would have been more effective to allow non-profit organizations or evangelical organizations to build their own MFI without being encumbered by large existing infrastructure.

   b) **Rupee Transactions:** All transactions must be done only in India’s national currency, the rupee. While this may not be a threat in the beginning, this may pose a constraint for interoperability between Indian mobile payments and the world. Also, it excludes providers from the lucrative remittance market in India and limits areas from which mobile operators can be profitable.

c) **Existing Account Holders:** The guidelines also state that only those having a valid bank account would be allowed mobile banking. This limits the full potential of mobile banking to extend micro-credit and bring banking to the large number of unbanked customers in India.

C. **Demographic Challenges:** India has 18 official languages which are spoken across the country. The state governments also are dictated to correspond in their regional language for official purposes. Additionally, two-thirds of the population in India is illiterate, creating difficulties in deployment of mobile banking solutions. For a pan-Indian mobile banking solution, this will be cumbersome to overcome.

SECURITY ISSUES IN MOBILE BANKING

Mobile banking has two zones, one is the handset held by the user and the other is the bank zone. Literature shows that possibility of security threat exists for transaction of payment using mobile device (Jin Nie and Xianling Hu. 2008).

a) **Wireless Application Protocol (WAP):** Wireless Application Protocol is used for communication between devices like digital mobile phones, internet, PDA etc. Through WAP customer can realize more functionality of internet banking. Encryption process is currently used for secure data transmission between bank and users but the problem is that this encryption process is not good enough for the protection of sensitive data between bank and customer. The reason is that security methods require more powerful computing and high storage capacity. If we take internet banking it is realized that there are powerful computer systems and well defined complex encryption process to ensure the security. Mobile device have low computational capacity and hence we are unable to apply complex cryptographic system (Jin Nie and Xianling Hu. 2008).

Due to advancement in technology, it is now necessary to provide end-to-end security. It means that if user uses his/her mobile device for mobile banking then the data transacted are secure at the bank end and not at the user end, thus leaving the data vulnerable to attacks. It was noted that it is difficult to provide end to end security through WAP. The reason is that the data is not encrypted at gateway during the switching of protocol process, which leads to security concern for mobile banking in WAP (Narendiran et. al., 2009).

b) **Authentication Risks and Issues:** One of the authentication method used in mobile banking is the login method. However PINS authentication method is an old method and many security issues such as password and id theft were discovered in this method. In such cases, the secret may be revealed and this results in customer's distrust on the security service company. Bank follows some security mechanisms in mobile banking. While the customers and the banks are bound to each other. This security mechanism is done by identifying the customer's phone number, SIM card number, pin number etc. Customer likes to use the mobile banking technology because of its mobility as they can access the bank anywhere and in any situation. They can transfer their money from one account to another account faster in a user-friendly environment. And also they can check the current status of their account. But all customers of the bank are not ready to use this service because of some security issues. They are not ready to adopt the mobile banking systems as it brings inconvenience to the users assuming that it cannot prevent direct or indirect attacks (Bilal and Shanker, 2011).

c) **SMS based Mobile Banking:** SMS based mobile banking is a convenient and easy way for accessing bank but there are end-to-end security problems. These problems exist in SMS, GPRS protocols and security issues for transaction of money. Today, most of the banks in the world offer SMS based mobile banking. If we take any mobile banking system we can realize that customers also interact with databases, files and important records through mobile phone. Currently South Africa, Bangladesh and some other countries are also doing SMS based mobile banking (Narendian et. al., 2009).

d) **Virus Attacks in mobile banking:** There are more than fifty thousand different types of computer viruses, internet malicious program and Trojans (Wilson, 1999). Software like Trojan horses can easily take up password on the web browser or any cached information on operating system. Malicious codes are written for remote communication.

e) **Risk with Digital Signature:** To reduce hardware cost, designer may prefer digital signature. Digital signature is efficient that’s why most companies are interested in digital signature for authentication. It is founded that digital signature is computational intensive. With unsigned values for example date, amount, they differed from transaction to transaction. So a signed template can be used with several unsigned values like date, amount etc. (Amir, 2003).

RECOMMENDATIONS

On the basis of key findings of the study following recommendations on security issues were made:

1. Mobile phones used for Mobile Banking could be easily hacked remotely, posing security threat. To address this, banks should execute restricted functionality option while providing Mobile Banking services. Pande (2009) suggested that due to this restricted functionality user needs to apply for adding a new payee or for increasing payment limit thus preventing the initiation of unauthorized payments from the user’s mobile phone remotely.
2. Further to manage remote hacking of mobile and subsequent fraud; one-time password (OTPs) should be used. When a request is received, a password is sent to the user’s phone via SMS. This password is expired once it has been used or once its scheduled life-cycle has expired.
3. Still many banks are using less than 128 bit SSL (Secure Socket Layer) encryption in Mobile Banking, which poses risk of data transmitted over the air being intercepted. RBI should make it mandatory for banks to apply at least 128 bit SSL encryption. Further to add in security banks should opt for VeriSign verification.
4. Many a time mobile phones engaged in wireless access protocol (WAP) based Mobile Banking, lack personal firewalls which may pose security threat. Here banks should try to build customer awareness regarding use of firewall, regular updation of antivirus program in mobile phones.

5. Mobile Banking is not much secured against potential threats of malicious code, phishing and SMiShing. To make it secure against malicious codes users must be made aware about use of antivirus and antimalware program in JAVA enabled phones and smart phones. Again to protect users from the threat of phishing and SMiShing consumer awareness in the key.
6. There is a fear that recent increase in 'fund transfer limit without end to end encryption for banks' by RBI from Rs.1000 to Rs. 5000; may lead to increase in fraudulent cases. This issue should be addressed very prudently as there is tradeoffs for increased security, mainly higher operational cost to banks.
7. Real Time Notification (RTN) after any Mobile Banking transactions should be made mandatory so as to quickly inform customers of suspicious or potentially fraudulent activities and empower them to immediately take action.

CONCLUSION

As mobile technology could be a growing technology in banking, finance and commerce sector by that we will save our time and might access our account and data of our account from anyplace and anytime and it additionally keeps alert us with our account group action and with alternative necessary data. however there is some security connected risk and challenges might return to beat these risk and challenges we have to enhance our security system and improve the authentication system for secure services and build trust in customer to use of mobile banking services and can take away barrier in adoption of mobile banking services.

Security around the transfer of data through communication channels is a challenge for developers, they noted, pointing out that developers are placing too much confidence in secure end-user behavior and back-end server-side communications. Even now many customers are uncomfortable with online banking regarding with security. In addition to that cyber criminals are trying day by day to find new techniques to avail unauthorized access to finances of financial institutions, banking customers. In developing countries, electronic crime is a serious problem because there is a lack of training on the subjects to investigate the electronic crime. Precaution is the only way to maintain secured transactions in this mobile banking system. There is a need to bring changes in the Information Technology Act to make it more effective to fight cyber crime. Mobile banking services play a significant role in improving customer satisfaction in high level and it has its own impact on customer satisfaction.

REFERENCES

- Agarwal, Gaurav (2007). Financial Inclusion through Mobile Phone Banking: Issues and Challenges. Cab Calling, July-September issue, 2007.
- Amarnani, Shalini (2009). Feature – Mobile Banking in India. http://www.cashcow.in/?p=580 (accessed on Oct 30, 2009).
- Ashta, A. (2010). Evolution of Mobile Banking Regulations. http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=473010 (accessed on Oct 23, 2010).
- Ba, S., Pavlou, P. A. (2002). Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior. MIS Quarterly, 26(3), 243-268.
- Bamoriya, P., Bamoriya, H., Singh, P. (2013), Perceptual mapping of electronic banking channels in India: A Multidimensional Scaling approach, International Journal of Research Studies in Management, 4(1).
- Bamoriya, Prerna Sharma, Singh, P. (2011). Issues & Challenges in Mobile Banking In India: A Customers' Perspective. Research Journal of Finance and Accounting. http://iiste.org/Journals/index.php/rjfa/article/view/189/73 (accessed on July 31, 2011).
- Bhatnagar, A., Misra, S., Rao, H. R. (2000). On Risk, Convenience, and Internet Shopping Behaviour. Communications of the ACM, 43(11), 98-105.
- Bueno, Manuel (2008). An Overview of the Mobile Phone Banking Industry. IE Publishing, 4-15
- Chen, L. D. (2006). A Theoretical Model of Consumer Acceptance Of mPayment. http://aisel.aisnet.org/amcis2006/247 (accessed on June 4, 2009).
- Cheney, J. S. (2008). An Examination of Mobile Banking and Mobile Payments: Building Adoption as Experience Goods? www.philadelphia.org/pcc. (accessed on Aug 22, 2009).
- Dasgupta, P. (2013). Mobile Banking: An Introduction, http://www.streetdirectory.com/travel_guide/133638/phones/mobile_banking__an_introduction.html (accessed on Sep 11, 2013).
- Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. http://www.jstor.org/pss/249008 (accessed on March 11, 2010).
- Epstein, Keith, Smith, Geri (2007). The Ugly Side of Microlending. BusinessWeek, Dec 13, 2007.
- Fain, D., Roberts, M. L. (1997). Technology vs. Consumer Behaviour: the Battle for the Financial Services Customer. Journal of Direct Marketing, 11(1), 44- 54.
- Gartner (2009). Gartner Report. http://www.gartner.com/it/page.jsp?id=1224645 (accessed on Jan 02, 2011).
- Gupte, L. (2008). Affordability Key in Bringing Digital Inclusion, Realizing the Potential of Mobile Banking. Horizons expanding, issue Jan/2008.
- Hannes, van R. (2011). KYC for Mobile Banking in Emerging Markets. http://mbanking.blogspot.com/2011/04/kyc-for-mobile-banking-in-world-of.html (accessed on May 12, 2011).
- Jacobsen, K., Landau, L. (2003). The Dual Imperative in Refugee Research: Some Methodological and Ethical Considerations in Social Science Research on Forced Migration. Disasters, 27(3), 185-206.
- Jarvenpaa, S. L., Todd, P. A. (1996). Consumer Reactions to Electronic Shopping on the World Wide Web. International Journal of Electronic Commerce, 1(2), 59-88.
- Moni, V. S. (2010). Mobile Banking in India. http://www.articlesbase.com/communication-articles/mobile-banking-in-india 2965902.html (accessed on Jan 22, 2011).
- Rao, G. R., Prathima, K. (2003). Online banking in India. Mondaq Business Briefing, April issue, 67-88.

- Vijayasarathy, L. R. (2002). Internet Taxation, Privacy and Security: Opinions of the Taxed and Legislated. Quarterly Journal of Electronic commerce, 3(1), 53-71.