Mobile Banking in India: Imperative and Challenges

Dr. RANJANA SHARMA
Associate Professor
Faculty of Management
Sri Guru Ram Rai Institute of Science and Technology (SGRRITS),
Dehradun (UK)

ABSTRACT

Technology plays an important role in banking sector. Banking is one of the largest financial institutions constantly explores the opportunity of technology enabled services to provide better customer experiences and conveniences. Mobile banking (also known as M-banking, sms banking) is a term used for performing balance checks, account transactions, payments etc. via a mobile device such as mobile phone. The increased prevalence of mobile phones provides exciting opportunities for the growth of mobile banking (m-banking). These papers are classified into five main categories: m-banking overview and conceptual issues, Features & Benefits of Mobile Banking, Current operating practices of commercial banks, Mobile banking/payment practices in Indian Commercial Banks and Challenges in India strategic, legal and ethical issues.

Key Words: Banking and Mobile Services, Customer, Issues, Mobile Banking, Challenges.

1. INTRODUCTION

Twelve billion people are expected to own mobile phones in the globe by 2015 (Mobile economy, 2015). There are currently 475 million mobile phones in India and 148 million are added every year. In a few years more than 790 million people are expected to have mobile phones in India (Peterson, 2009).

Mobile commerce is a natural successor to electronic commerce. The capability to pay electronically coupled with a website is the engine behind electronic commerce. Electronic commerce has been facilitated by Automatic Teller Machines (ATMs) and shared banking networks, debit and credit card systems, electronic money and stored value applications and electronic bill presentment and payment systems (Ashta, 2010). Mobile payments are a natural evolution e-payment schemes that will facilitate mobile commerce. A mobile payment or m-payment may be defined, for our purposes, as any payment, where a mobile device is used to initiate, authorize and confirm an exchange of financial value in return for goods and services (Barnes and Corbitt, 2003). Mobile devices may include mobile phones, PDAs, wireless tablets and any other device that connect to mobile telecommunication network and make it possible for payments to be made (Clark, 2008). The realization of mobile payments will make possible new and unforeseen ways of convenience and commerce. Unsuspected technological innovations are possible (Amir, 2003).

In this paper we present an overview of the mobile technology landscape and address the concomitant issues that arise with the introduction of mobile payment services.

2. BENEFITS OF MOBILE BANKING

A mobile payment service in order to become acceptable in the market as a mode of payment the following conditions have to be met:

a) **Simplicity and Usability**: The m-payment application must be user friendly with little or no learning curve to the customer. The customer must also be able to personalize the application to suit his or her convenience.
b) **Universality:** M-payments service must provide for transactions between one customer to another customer (C2C), or from a business to a customer (B2C) or between businesses (B2B). The coverage should include domestic, regional and global environments. Payments must be possible in terms of both low value micro-payments and high value macro-payments.
c) **Interoperability:** Development should be based on standards and open technologies that allow one implemented system to interact with other systems.
d) **Security, Privacy and Trust:** A customer must be able to trust a mobile payment application provider that his or her credit or debit card information may not be misused. Secondly, when these transactions become recorded customer privacy should not be lost in the sense that the credit histories and spending patterns of the customer should not be openly available for public scrutiny. Mobile payments have to be as anonymous as cash transactions. Third, the system should be foolproof, resistant to attacks from hackers and terrorists. This may be provided using public key infrastructure security, biometrics and passwords integrated into the mobile payment solution architectures (Pandey, 2012).
e) **Cost:** The m-payments should not be costlier than existing payment mechanisms to the extent possible. A m-payment solution should compete with other modes of payment in terms of cost and convenience.
f) **Speed:** The speed at which m-payments are executed must be acceptable to customers and merchants.
g) **Cross border payments:** To become widely accepted the m-payment application must be available globally, word-wide.

3. ADVANTAGES OF MOBILE BANKING

A very effective way of improving customer service could be to inform customers better. Credit card fraud is one such area. A bank could, through the use of mobile technology, inform owners each time purchases above a certain value have been made on their card. This way the owner is always informed when their card is used, and how much money was taken for each transaction.

Similarly, the bank could remind customers of outstanding loan repayment dates, dates for the payment of monthly installments or simply tell them that a bill has been presented and is up for payment. The customers can then check their balance on the phone and authorize the required amounts for payment.

The customers can also request for additional information. They can automatically view deposits and withdrawals as they occur and also pre- schedule payments to be made or cheques to be issued. Similarly, one could also request for services like stop cheque or issue of a cheque book over one’s mobile phone.

There are number of reasons that should persuade banks in favor of mobile phones. They are set to become a crucial part of the total banking services experience for the customers. Also, they have the potential to bring down costs for the bank itself. Through mobile messaging and other such interfaces, banks provide value added services to the customer at marginal costs.

Such messages also bear the virtue of being targeted and personal making the services offered more effective. They will also carry better results on account of better customer profiling (Soni, 2010)

Yet another benefit is the anywhere/anytime characteristics of mobile services. A mobile is almost always with the customer. As such it can be used over a vast geographical area. The customer does not have to visit the bank ATM or a branch to avail of the bank’s services. Research indicates that the number of footfalls at a bank's branch has fallen down drastically after the installation of ATMs. As such with mobile services, a bank will need to hire even less employees as people will no longer need to visit bank branches apart from certain occasions. With Indian telecom operators working on offering services like money transaction over a mobile, it may soon be possible for a bank to offer phone based credit systems. This will make credit cards redundant and also aid in checking credit card fraud apart from offering enhanced customer convenience. The use of mobile technologies is thus a win-win proposition for both the banks and the bank's customers (Sharma & Singh, 2011).

The banks add to this personalized communication through the process of automation. For instance, if the customer asks for his account or card balance after conducting a transaction, the installed software can send him an automated reply informing of the same. These automated replies thus save the bank the need to hire additional employees for servicing customer needs (Nandhi, 2012).

4. CURRENT OPERATING PRACTICES OF COMMERCIAL BANKS IN INDIA

[A]. Activities and Primary Functions of Commercial Banks - Deposit Acceptance: Being a short term credit dealer, the commercial banks accept the savings of public in the form of following deposits. [Mobile Payment Forum of India (MPFI)]

- ❖ Fixed term deposits
- ❖ Current A/c deposits
- ❖ Recurring deposits
- ❖ Saving A/c deposits
- ❖ Tax saving deposits
- ❖ Deposits for NRIs

a) **Lending Money:** A second major function is to give loans and advances and thereby earn interest on it. This function is the main source of income for the bank. Overdraft facility: Permission to a current A/c holder of withdrawal more than to what he has deposited.

b) **Loans & advances:** A kind of secured and unsecured loans against some kind of security. Discounting of bill of exchange: in case a person wants money immediately, he/she can present the B/E to the respective commercial bank and can get it discounted.

c) **Cash credit:** Facility to withdraw a certain amount of money on a given security.

[B]. Secondary Functions of Commercial Banks - Agency functions: Bank pays on behalf of its customers as an agent and gets paid fee for agency functions such as:

- ❖ Payment of taxes, bills
- ❖ Collection of funds through bills, cheques etc.
- ❖ Transfer of funds
- ❖ Sale-purchase of shares and debentures
- ❖ Collection/Payment of dividend or interest
- ❖ Acts as trustee & executor of properties
- ❖ Forex Transactions
- ❖ General Utility Services: locker facility

Credit Creation: It is one of the most outstanding functions of commercial banks. A bank creates credit on the basis of its primary deposits. It further lends the money which people has deposited with the bank also charge interest on this money, which is much higher than what it actually pays to depositor. Thus bank generates money for itself.

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

   i. **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.

   ii. **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.

   iii. **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.

6. 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).

7. RECOMMENDATIONS

This paper shows 'mobile handset operability' is an important issue in mobile banking, due to availability of various handset models (supporting different type of technology) in the market. To resolve it service providers *i.e*. banks must coordinate with mobile handset manufacturers so that all handsets irrespective of manufacturer and technology (GSM or CDMA) become compatible with single mobile banking technology.

Majority customers perceived 'privacy and security' a critical issue. Here banks are advised to educate customers on this issue to raise their awareness. Especially for the customers' worries like losing money if once mobile handset is lost (substantial number of respondents worried about it). Secondly banks and telecom operators are suggested to draft comprehensive joint policy regarding security & privacy so that customers can be assured at both banks and telecom operator's levels while doing mobile banking.

'Standardization' is another major issue as lack of standardization of mobile banking services in the country resulted in increased complexity while using mobile banking services (especially when using mobile banking services of multiple banks). For resolving this issue banks are advised to developed mobile banking standards in guidance of RBI.

Issues of 'download & installation of application s/w', 'customization' (user's preferred language) and 'telecom service quality' were not perceived critical or important. Reason may be that study was conducted in urban area so technological aspect of application s/w, absence of local/preferred language and telecom service quality like network unavailability were not perceived as major issues. But banks are well advised not to overlook above issues as these may be critical in pan India adoption of mobile banking.

REFERENCES

1. Amir Herzberg (2003). Payments And Banking With Mobile Personal Devices and Communications. *ACM*, Vol. 46 (5), p-45-47.
2. Ashta, A. (2010). Evolution of Mobile banking Regulations. JIBC, Vol 10 (7), pp – 12-16.
3. Bilal, M. and Sankar, G. (2011). "Trust & Security issues in Mobile banking and its effect on Customers. *Karlskrona Sweden*, Vol. 10 (4), pp.371-379.
4. Barnes, S. J., and Corbitt, B. (2003). Mobile Banking: Concept and Potential. *International Journal of Mobile Communications*, Vol.1 (3), pp. 273-288.
5. Brown, I., Cajee, Z., Davies, D. and Stroebel, S (2003). Cell phone banking: predictors of adoption in South Africa-an exploratory study. *International Journal of Information Management*, Vol.23 (10), pp. 381-394.
6. Clark, A. (2008). Mobile banking &Switching. Retrieved from www.mcom.co.nz.
7. Devadevan, (2013). Mobile banking in India, *International Journal of Emerging Technology and Advanced Engineering*, Vol. 3 (6), pp – 56-61.
8. Jin Nie and Xianling Hu. (2008) Mobile Banking Information Security and Protection Methods. *International Conference on Computer Science and Software Engineering,* pp. 587-590.
9. Mobile Payment Forum of India (MPFI) http://www.mpf.org.in.
10. Nandhi. M. A. (2012)., Effects of Mobile Banking on the Savings Practice of Low Income Users – The Indian Experience, Institute for money technology and financial inclusion, working paper.
11. Narendiran, C., Rabara, S and Rajendran, N (2008). Performance evaluation on end-to-end security architecture for mobile banking system. *Wireless Days,* pp. 1-5.
12. Pandey, G.B. (2012). Mobile Banking in India: Practices,Challenges and Security Issues. *International Journal of Advanced Trends in Computer Science and Engineering*. Vol. 1 (2), pp-34-39.
13. Sharma, P. and Singh, P. (2009). Users' perception about mobile banking- with special reference to Indore & around. *Review of Business & Technology Research*, Vol. 2 (1), pp-1-4.
14. Soni, P. (2010). M-Payment Between Banks Using SMS. *Proceedings of the IEEE*, Vol. 98 (7), pp. 903-905.
15. Wilson, T (1999). Malicious mobile. *Internet Business*, Vo. 2 pp. 52-53.

List of Abbreviations

AML - Anti Money Laundering
CDMA - Code Division Multiple Access
GPRS - General Packet Radio Service
GSM - Global System for Mobile
IDS - Intruder Detection System
IRDA - Infrared Data Association
ISO - International Standards Organization
IVR - Integrated Voice Response
KYC - Know Your Customer
MNO - Mobile Network Operator
mPIN - Mobile Personal Identification Number
MPFI - Mobile Payment Forum of India
NFC - Near Field communication.
OTP - One Time Password
PCI-DSS - Payment Card Industry Data Security Standard
PIN - Personal Identification Number
RFID - Radio Frequency Identification
SIM - Subscriber Identity Module
SMS - Short Messaging Service
USSD - Unstructured Supplementary Service Data
WAP - Wireless Application Protocol