CONTEMPORARY ISSUES OF M – COMMERCE IN RECENT SCENARIO

Dr.C. Manikanda Muthukumar*   R.D. Geetha**

Assistant Professor & Research Guide, PG and Research Dept. of Commerce, Government Arts College (Autonomous) Salem, India.

Research Scholar, PG and Research Dept. of Commerce, Government Arts College (Autonomous) Salem, India.

Abstract

The increased prevalence of mobile phones provides exciting opportunities for the growth of mobile banking (m-banking). This paper reviews the emerging based on 65 m-banking papers published between2000 and mid-2010 in Information Systems (IS), technology innovation, management, and marketing journals, and major IS conferences. 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 inIndia strategic, legal and ethical issues.

Key Words: Banking and Mobile Services, Customer, Issues, Mobile Banking, India, M-Banking, Challenges of M-Banking in India.

1. INTRODUCTION

Three billion people are expected to own mobile phones in the globe by 2012. There are currently 225 million mobile phones in India and 100 million are added every year. In a few years more than 500 million people are expected to have mobile phones in India. 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. Mobile payments are a natural evolution e - payment schemes that will l 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. 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. The realization of mobile payments will make possible new and unforeseen ways of convenience and commerce . Unsuspected technological innovations are possible are possible.

Several mobile payment companies and initiatives in EU have failed and many have been discontinued. In Europe and North America with few exceptions such as Austria, Spain and Scandinavian countries the development of mobile payments has not been successful. However, mobile payment services in Asia have been fairly successful especially in South Korea, Japan and other Asian countries (e.g., Mobile Suica, Edy, Moneta, Octopus, and G Cash). NTT DoCoMo has 20 million subscribers and 1.5 million of them have activated credit card functionality in Japan. There are 100,000 readers installed in Japan. The main difference between successful implementations of mobile payment services in the Asia Pacific region and failure in Europe and North America is primarily attributed to the ‘payment culture’ of the consumers that are country-specific. 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. FEATURES & BENEFITS OF MOBILE BANKING (MOBILE PAYMENT CHARACTERISTICS)

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) 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.

d) **Cost**
The m-payments should not be costlier than existing payment mechanisms to the extent possible. An m-payment solution should compete with other modes of payment in terms of cost and convenience.

e) **Speed**
The speed at which m-payments are executed must be acceptable to customers and merchants.

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 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.

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.

3. REVIE OF CURRENT OPERATING PRACTICES OF COMMERCIAL BANKS IN INDIA

3.1 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:

- Fixed Term Deposits
- Current A/C Deposits
- Recurring Deposits
- Saving A/C Deposits
- Tax Saving Deposits
- Deposits For NRIs

Lending Money:A second major function is to give loans and advances and there by 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.

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.

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

3.2 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 bulk generates money for itself.

List of Abbreviations

- AML Anti Money Laundering
- CDMA Code Division Multiple Access
- GPRS General Packet Radio Service
- 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

4. CHALLENGES WITH ADOPTION OF MOBILE BANKING

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. Therefore, any mobile banking must be inexpensive enough to be attractive for the end-customer over existing methods.

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

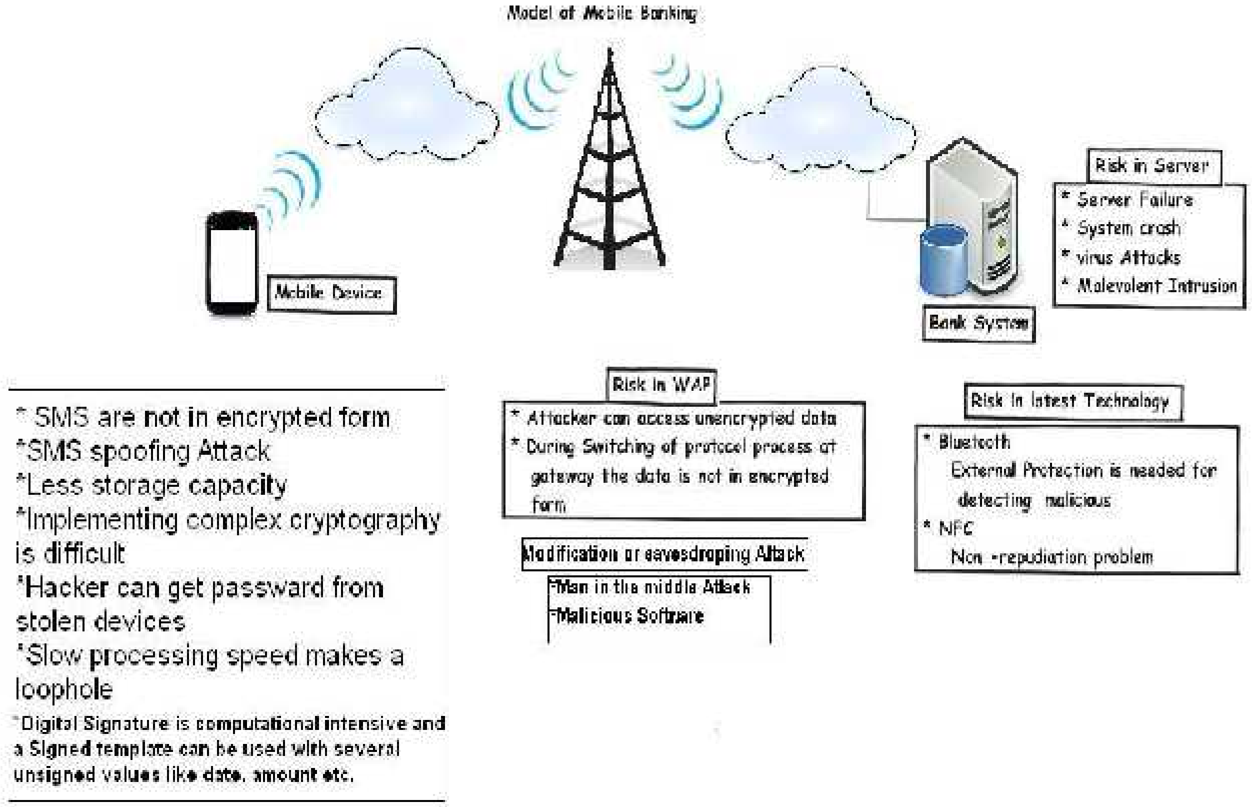
The guidelines also state that only those having a valid bank account would be allowed mobile banking. This limits the full potential of mobile banking to extend micro-credit and bring banking to the large number of unbanked customers in India.

5. MOBILE BANK TRANSACTION SERVICES MODE

5.1 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.

5.1.1 Mobile banking and Security issues with WAP (Wireless Application Protocol)


Model of Mobile Banking
Mobile Device
Bank System
Risk in Server
* Server Failure
* System crash
* virus Attacks
* Malevolent Intrusion
Risk in WAP
* Attacker can access unencrypted data
* During Switching of protocol process at gateway the data is not in encrypted form
Modification or eavesdroping Attack
-Man in the middle Attack
-Malicious Software
Risk in latest Technology
* Bluetooth
External Protection is needed for detecting malicious
* NFC
Non -repudiation problem
* SMS are not in encrypted form
*SMS spoofing Attack
*Less storage capacity
*Implementing complex cryptography is difficult
*Hacker can get passward from stolen devices
*Slow processing speed makes a loophole
*Digital Signature is computational intensive and a Signed template can be used with several unsigned values like date, amount etc.

WAP 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 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 .

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.

5.1.2 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 we are 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.

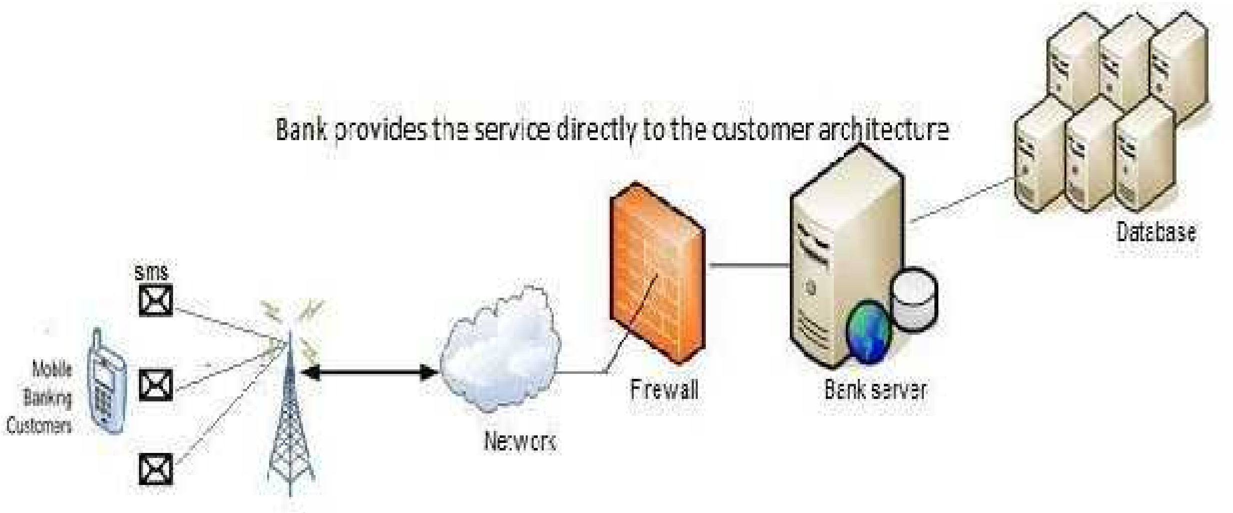
They can transfer their money from one account to another account faster in a user- friendly environment. And also they can check the current status of their account. But all customers of the bank are not ready to use this service because of some security issues. They are not ready to adopt the mobile banking systems as it brings inconvenience to the users assuming that it cannot prevent direct or indirect attacks.

Authentication Model

There are two types of services provided to the customer which are as follows:

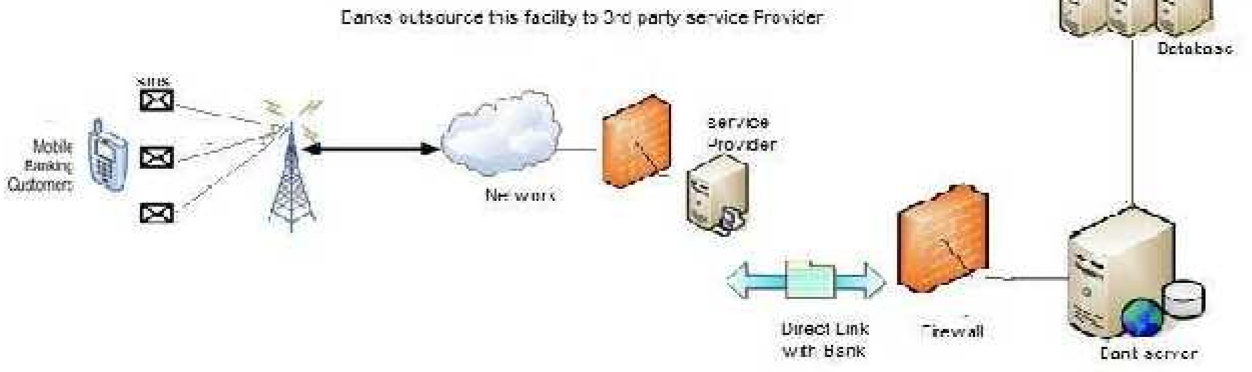
I. The bank provides the service directly to the customer.
II. Banks share their facility to 3rdparty service provider.

5.1.3 Bank provides the service directly to the customer Architecture


Bank provides the service directly to the customer architecture
sms
Mobile Banking Customers
Network
Firewall
Bank server
Database

Provides the service directly to customer Architecture. This is a setup which shows the Internet web server, database, application server and firewall architecture is an example of mobile banking service handled directly by the bank. In this application, server plays an important role to provide services to the customer. The database will be accessed by transactions both from the bank and from mobile device. If a customer wishes to process the transaction, for example, transaction of money from one account to another account he/she must first authenticate themselves to the server through firewall. And the security application at the server has to verify the user through password or pin number and the server allows the customer to do transactions. In this method, there are some security issues such as server failure, system crash and malevolent intrusion. These are serious problems and will not make the server come back in normal form. So many banks do not prefer this method.

5.1.4 Banks share their facility to 3rdparty service provider



Familiar banks outsource their facility to 3r d party architecture i.e. handling mobile banking customer service to 3r d party service provider. This service provider may lie close to the bank geographically or it may be in other country. They handle the customer through mobile or internet. They are responsible for secure transaction and management of the customer data. This method also has authentication issues as they follow the same authentication method like verifying the pin or password with the database and it also involves 3r d party server. There is no trust in securing the data of customers such as bank account details and customer addresses as they are managed by 3rd party service provider. So customer feels no security to their password and details to the unknown 3rd party. And also customers need to pay extra charge for their service. This is a list of issues that need to improve by the 3rd party.

- Network Security & Control
- Parental Controls
- Customer Privacy & Informed permission
- Liability
- Fraud Prevention (or)
- Authentication Interoperability (or)
- Standardization Data Access &
- Use Financial Risks (or) Reward

5.1.5 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. Currently in South Africa the standard bank uses WIG and FNB bank uses SMS based approach for mobile banking. In this scenario, the user sends PIN number to the bank's server and then the server is ready for accepting the requests. This approach is not fully secure because the data is transmitted and the network operator has full access to the data.

5.1.6 SMS encryption

As default data format for SMS is plaintext. Currently end to end encryption is not available. The only encryption involved at base transceiver station and SMS bank server during transmission. The encryption algorithm used is A5 which is proven to be defenseless.

5.1.7 SMS Spoofing Attack

The most dangerous attack in SMS banking is spoofing attack where attacker can send messages on network by manipulating sender's number. Due to spoofing attack, most of the organizations are not adopting mobile banking through SMS.

5.1.8 Virus Attacks in mobile banking

There are more than fifty thousand different types of computer viruses, internet malicious program and Trojans. 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. Zeus Trojan targeted mobile bank users. Zitmo has been used by attackers to defect SMS banking. Zeus is commonly used to steal mobile transaction Authent number or password.

5.1.9 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.

6. REVIEW OF THE LITERATURE

Barnes and Corbett ; Scornavacca and Barnes (2004) suggest that recent innovations in telecommunications have enabled the launch of new access methods for banking services, one of these is mobile banking; whereby a customer interacts with a bank via a mobile device such as a mobile phone or personal digital assistant. Karjaluoto *etal*.; Rugimbana (1995) found that there is vast market potential for mobile banking due to its always-on functionality and the option to do banking virtually any time and anywhere. Unnithan and Swatman [34] studied the drivers for change in the evolution of the banking sector, and the move towards electronic banking including mobile banking by focusing on two economies, Australia & India and suggested strong growth potential of new banking channel in India. Clark (2008) suggests that as a Channel the mobile phone can augment the number of channels available to consumers, thereby giving consumers more low-cost self service options by which to access funds, banking information and make payments. Mobile as a channel delivers convenience, immediacy and choice to consumers. Vyas (2009); Raoetal suggest banks will need to expand their thinking about mobile banking beyond online banking and should start to view mobility as its own powerful and compelling delivery channel that can help them deliver to end users new value such as immediate access and additional control of personal finances. According to Vyas (2009) Banks will target non-online banking users who may lack regular access to desktop Internet but are very likely to own a mobile device. Gupta (1999); Pegu (2000); Dasgupta (2002) also affirms future of mobile banking in India in their studies. Suorant found that the average mobile banking user is married, 25 to 34 years old, has intermediate education and average income in clerical work. She found that age and education have a major influence on the use of the mobile phone in banking services. The adoption theories assume that use of Internet banking precedes the adoption of the mobile phone in banking. However, Suoranta [30] found that some mobile banking customers omit Internet banking adoption when adopting the mobile phone for banking actions. The study is aimed to evaluate perceptions and opinions of urban mobile banking users. For this a cross sectional descriptive design was adopted with ad-hoc quota sampling. Sample was comprised of 50 mobile banking users and 50non-users of Ghaziabad city, India. Non-users were defined as individuals having bank account but not using mobile banking. Of the total respondents students were 68.18%; remaining were working. 24.4% respondents were graduates and 75.6% were postgraduates. Data was obtained by using structured questionnaire. Data was screened for missing values (available case method was adopted to handle missing values) and outliers. Data was further subject to normality- data was found to be normally distributed as skew index ranged from (reference (reference absolute value 10). This questionnaire was analyzed for scale reliability analysis which suggests that items makeup the scale measured the same underlying constructs, as cronbach's alpha coefficient was found convergent validity was confirmed as significant correlation (moderate to large, sig .05) was present between items measuring single construct. Study 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 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.

10. CONCLUSION

The Mobile Payment Forum of India (MPFI) has been formed with Institute for Development and Research in Banking Technology (IDRBT) and Rural Technology Business Incubator (RTBI), IIT Madras taking the lead role. It has member s and representatives from the telecommunications industry, financial institutions (banks and microfinance institutions) as well members from the Reserve Bank of India. Three sub- committees have been formed – on technology, on business models and on regulatory issues. The first meeting of MPFI was held in Hyderabad on the 15th of September 2007. The subcommittees are expected to go over their particular concerns in depth and submit a report shortly. Lots of challenges are to be overcome for a successful implementation of mobile payments to be widely accepted as a mode of payment. Businesses, merchants and consumers have to come forward and make value-producing investments. A regulatory framework and widely accepted standards will be the pillars on which mobile payment applications will be built. Research so far has outlined a diversity of thinking and innovation that exists in the m- payments arena. Numerous solutions have been tried and failed but the future is promising with potential new technology innovations.

REFERENCES

1. Amir Herzberg. Payments And Banking With Mobile Personal Devices, Communications of the ACM, issues, *www.* public.webfoundation.org/…... / 25, Mobile_banking_M-commerce_15.03.pdf, 2010.
2. Barnes,S.J., and Corbitt, B. Mobile Banking: Concept and Potential, International Journal of Mobile Communications, 1 (3), pp. 273-288, 2003.
3. C. Narendiran, S. Albert Rabara, and N. Rajendran. Public key infrastructure for mobile banking security, Global Mobile Congress 2009, pp. 1-6,2009.

4. C. Narendiran, S. Rabara, and N. Rajendran, ―Performance evaluation on end- to-end security architecture for mobile banking system, ‖ *Wireless Days, 2008. WD'08. 1st IFIP*, pp. 1-5,2008.
5. Dai Wei and Tang Yanling. Research on Security Payment Technology Based on Mobile Mobile E- Commerce, e-Business and Information System Security (EBISS), pp.1- 4,2010.
6. F. de la Puente, S. Gonzalez, and J. Sandoval. Virus attack to the PC bank, Security Technology Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference , pp. 304-310,1999.
7. H. Harb, H. Farahat, and M. Ezz. SecureSMSPay: Secure SMS Mobile Payment model, Anti - counterfeiting, Security and Identification ASID, pp. 11- 17,2008.
8. H. Wu, A. Burt, and R. Thurimella. Making secure TCP connections resistant to server failures, Computer Security Applications Conference 2003, Proceedings.19th Annual, pp. 197-206,2003.
9. Jin Nie and Xianling Hu. Mobile Banking Information Security and protection Methods, Computer Science and Software Engineering, 2008,International Conference , pp. 587-590, 2008.