Mobile Banking in India: Practices,Challenges and Security Issues

Vishal Goyal[1] , Dr.U.S.Pandey[2], Sanjay Batra[3]
[1] Research Scholar Singhania University, vishalgoyal9673@gmail.com
[2.]Open Learning, Delhi University, uspandey1@gmail.com
[3]Research Scholar Manav Bharti University

ABSTRACT

The increased prevalence of mobile phones provides exciting opportunities for the growth of mobile banking (m-banking). This paper reviews the emerging research literature on m-banking. It presents a classification framework for m-banking research based on 65 m-banking papers published between 2000 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 in India strategic, legal and ethical issues. It is expected that the comprehensive list of references and assessments presented in this paper will provide a useful anatomy of young m-banking literature to anyone who is interested in m-banking and help stimulate further interest.

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 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.

Music, video on demand, location based services identifiable through mobile handheld devices – procurement of travel, hospitality, entertainment and other uses are possible when mobile payments become feasible and ubiquitous. Mobile payments can become a complement to cash, cheques, credit cards and debit cards. It can also be used for payment of bills (especially utilities and insurance premiums) with access to account-based payment instruments such as electronic funds transfer, Internet banking payments, direct debit and electronic bill presentment.

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 GCash). 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) **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.
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.

2.1 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.

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.

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

3. REVIEW 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[20]:

- 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 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.

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 bank generates money for itself.

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 (Some times also written as International Organization for Standardization)
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.

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.
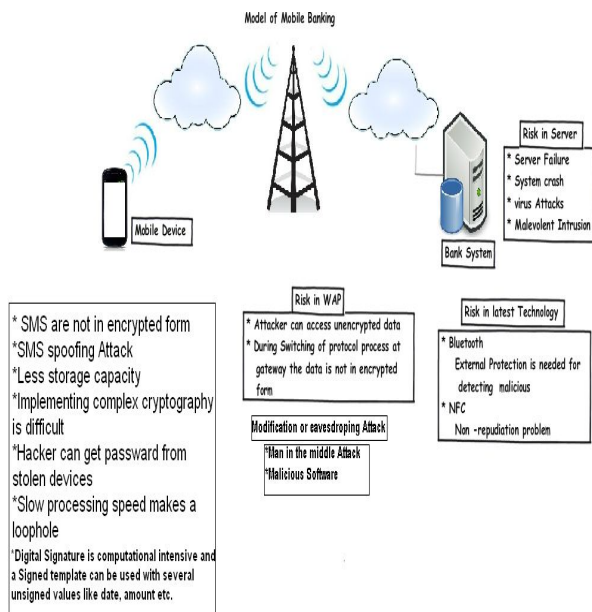
5. MOBILE BANK TRANSACTION SERVICES MODEL

Figure 1: Risks in mobile bank services for the customers

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 [16].

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

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 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 [16].

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 [6].

In China, mobile communication group introduced the ―China Mobile Communication and Information Resources station entities and Internet short Message Gateway Interface Protocol. It was noted that security is the susceptibility in WAP and that it is safe for the information to be delivered from the gateway to end user but due to accessibility of information for short time on gateway it may be possible for the attacker to access the information[9].

It is identified that users are not usually satisfied from mobile commerce over WAP. The reason is that, problems occur for reasons like low speed, unreliable connection, and high cost. A research on adaption of WAP services especially for mobile commerce market is in progress in countries like Hong Kong, China, Taiwan i.e. China economic region [28].

In South Africa, there are two technologies used for mobile banking namely WAP and WIG (Wireless Internet Gateway).

59

WIG is a short message service. For South Africa, security and cost are the most important issues in providing the service [15].

Table 1: Security threads for mobile banking

Risks identification related to Mobile banking	
Security issues	Mobile banking and security issues with Wireless Application protocol(WAP)
	Password for identification
	Password for identification third party enrollment in mobile banking application
	SMS based Mobile banking

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 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 [21].

The security mechanism adopted by the banks face many security issues like being attacked by unauthorized users which is of highest priority in terms of security. If the device gets stolen then the hackers or unauthorized persons may find the password from the log files or saved draft files. Many customers save their password in their mobile or they may keep the password under auto fill settings of the form, this loophole can be easily used by the unauthorized person. Uneducated people are less aware of these issues and thus leading to loss of trust by customers [31].

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

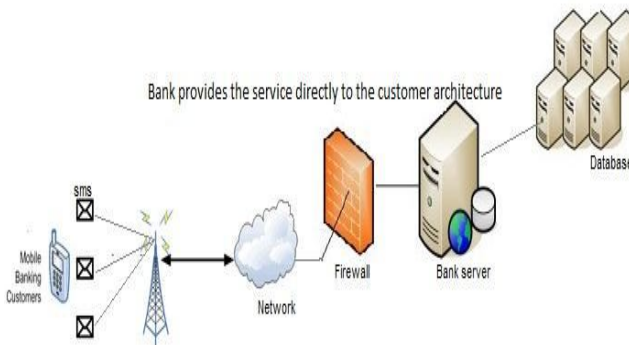### 5.1.3 Bank provides the service directly to the customer Architecture

Figure 2: Provides the service directly to customer Architecture

This is a setup which shows the Internet web server, database, application server and firewall at the bank's side. The above 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 mobile bank 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 bank 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 [10]. In this method, there are some security issues such as server failure, system crash, and malevolent intrusion [13]. These are serious problems and will not make the server come back in normal form. So many banks do not prefer this method.

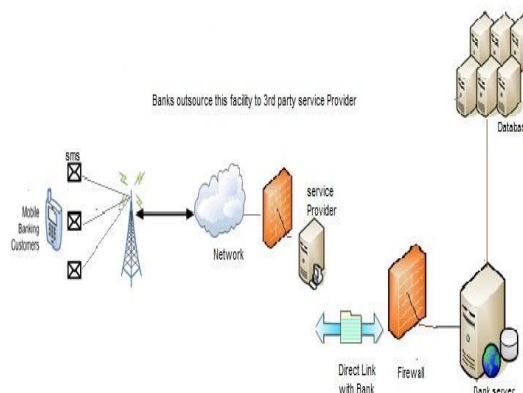### 5.1.4 Banks share their facility to 3rd party service provider

Figure 3: Banks share their facility to 3rd party service Provider

60

Familiar banks outsource their facility to 3rd party architecture i.e. handling mobile banking customer service to 3rd 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 3rd $party$ server. There is no trust [25] 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 share their password and details to the unknown 3rd party. And also customers need to pay extra charge for their service [35].

This is a list of issues that need to improve by the 3rd party service.

- 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 [7].

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 [6].

In Sri Lanka, mobile banking through SMS is gaining more popularity and the reason is that the cost of SMS is very low i.e. 2 Sri Lankan Rupees per SMS which is equal to 0.02 USD. News alert is also one of the popular SMS services in Sri Lanka. Pay Mate is a mobile payment

scheme in Sri Lanka. Ezy pay is another scheme of SMS banking through which users can do e-commerce activities. Research is ongoing to secure the SMS banking process [29].

In developing countries like Bangladesh SMS banking is gaining popularity because of low cost and low bandwidth requirement. The main advantages of SMS are the simplicity and easiness to use. Due to plain text property, SMS is not suitable for authentication. So lacking of privacy, integrity and security are the main issues involve in SMS banking [27]. SMS banking is useful for small consumer and for small merchant. SMS banking is also useful for travelers because customer can buy ticket for buses and trains easily and in urgent situations without going to the respective stations [22].

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 [7].

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 [12].

5.1.8 Virus Attacks in mobile banking

There are more than fifty thousand different types of computer viruses, internet malicious program and Trojans [33]. 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 [11]. Zeus Trojan targeted mobile bank users. Zitmo has been used by attackers to defect SMS banking. Zeus is commonly used to steal mobile transaction authentication number or password [32].

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 [2].

6. REVIEW OF THE LITERATURE

Barnes and Corbett [4]; 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 *et al*. [17]; 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); Rao et al. [26] 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. Suoranta [30] 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. Polatoglu et al. [23]; Al-Ashban and Burney [1]; Karjaluoto *et al*. [17]; Black *et al*. [5] supports findings of Suoranat in their respective studies. Mas [19]; Lyman et al. [18] found that there are a large number of different mobile phone devices and it is a big challenge for banks to offer mobile banking solution on any type of device. Some of these devices support J2ME and others support WAP browser or only SMS; presetting a serious challenge. Hayat [14] suggests that for a banking regulator it is important to provide adequate protection for consumers, ensure economic stability, provide interoperability of electronic systemms and guarantee security of transactions and Anti-Money Laundering and Know-Your-Customer principles must also be applied to mobile payments. Comninos et al. [8] suggest that unbanked will only transact electronically (online/mobile banking) if there is convenience and security. Sharma and Singh (2009) found that Indian mobile banking users are specially concern with security issues like financial frauds, account misuse and user friendliness issue - difficulty in remembering the different codes for different types of transaction, application software installation & updation due to lack of standardization. Banzal [3] found that another major issue is the revenue sharing agreements between mobile service providers, banks, content providers, aggregators and other service providers like utilities, travel agencies, hotel industry, retailers etc.

7. METHODOLOGY

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 50 non-users of Ghaziabad city, India. Non-users were defined as individuals having bank account but not using mobile banking. Of the total respondents 68.16 % were male and 31.84% were female. The sample was comprised of relatively young respondents. Of the total respondents students were 68.18%; remaining were working. 24.4% respondents were graduates and 75.6% were postgraduates [24].

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 -.29 to .46 (reference absolute value 3) and kurtosis index from -.1.91 to 2.05 (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 to be 0.764 (Annexure 1). At last convergent validity was confirmed as significant correlation (moderate to large, sig .05) was present between items measuring single construct.

Annexure 1

R E L I A B I L I T Y   A N A L Y S I S – S C A L E (A L P H A)
Reliability Coefficients   N of Class = 100.0   Alpha= .764

8. ANALYSIS AND DISCUSSION

Data was subject to Correlation analysis, Independent Samples T-test, ANNOVA, Percentile analysis.

8. 1 Mobile banking users: Demographic profile

Two-tailed Pearson Correlation was conducted to evaluate the relationship between mobile banking users and demographic variables viz. age, sex, education, occupation and income. Only demographic variable had significant correlation with user was sex (r=0.293, N=100, p<0.05, correlation strength moderate). Thus analysis suggests that males are more

inclined to use mobile banking in comparison to females (Table 2).

Table 2: Results of Correlation Analysis

Demographic variable	Correlation coefficient (N=100, p<0.05)
Age	0.067
Sex	0.293*
Education	-0.071
Occupation	-0.076
Income	0.031

8.2 Mobile banking users: Service usages pattern

Data was further subject to Percentile Analysis which suggested that among mobile banking users majority, 87.87 were availing mobile banking services from public/govt. banks. State Bank of India was largest mobile banking service provider overall followed by Punjab National Bank. Among private banks ICICI Bank was leading in mobile banking services (Table 3*)*. Percentile Analysis also suggested that majority of users were using services from less than 2 years and frequency of uses among majority of users was weekly (Table 4*)*.

Table 3: Mobile Banking Service usages pattern (a)

| Bank from which availing services	% Users

Public Banks
   1. SBI
   2. PNB
	87.87

Private Banks
   1. ICICI
   2. HDFC
	6.06

Both Public & Private Banks	6.06

Table 3: Mobile Banking Service usages pattern (b)

Mobile Banking Users			
Time Period	% of users	Frequency of use	% of users
Less than 6 months	39.39	Daily	24.24
6 months to 2 years	42.42	Weekly	45.45
More than 2 years	18.18	Monthly	30.3

8.3 Mobile banking users: Services preference

Data related to various mobile banking services in users were interested was also subject to Percentile Analysis to explore currently most preferred services in mobile banking.

Checking balance through mobile banking was most used service where as checking status of D.D. or cheque was least used. (Chart 1)

Chart 1: Mobile banking services preference
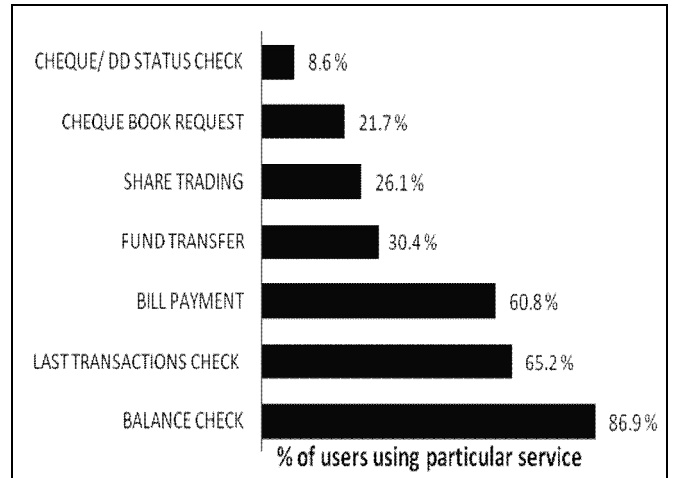
8.4 Mobile banking issues: Overall analysis

Overall Percentile Analysis was done for the responses of mobile banking users and non-users to explore selected issues in mobile banking which may impose challenges to service providers (banks), RBI, telecom operators etc. and thus may influence success of mobile banking in India (Table 4).

Table 4: Analysis of Mobile banking Issues

Level of agreement of the respondents (in % terms) with issues					
Mobile banking issues	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
Mobile handset operability	34.09%	47.27%	10.06%	6.81%	0.75%
Security / Privacy	27.77%	37.06%	20.10%	9.75%	5.30%
Standardization	15.90%	43.18%	24.24%	12.12%	4.54%
Downloading & Installing application software	10.63%	10.30%	33.33%	42.70%	3.02%
Customization	7.57%	26.06%	52.72%	12.12%	1.51%
Telecom Services Quality	10.09%	9.06%	43.93%	27.27%	9.60%

Analysis suggested that majority of respondents i.e. 81.36% strongly agree or agree that mobile handset operability is an issue in mobile banking as different types of handsets support different types of technology leading to

complexity. 64.83% respondents think that mobile banking is not secure, also data privacy is absent.

On standardization again majority 59.08 % respondents strongly agree or agree that mobile banking service standards are lacking among Indian banks which makes it difficult to do mobile banking from multiple service providers.

On the issues of download & installation of application s/w, customization (user's preferred language) and telecom service quality; majority of the respondents were either indifferent or disagree. 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.

8.5 Mobile banking issues: Users vs. non-users

One way ANOVA was applied to explore any significant difference in opinions of mobile banking users and non-users on selected issues in mobile banking. Results showed that there was no statistically significant difference in opinions of users and non-users for the selected issues (Annexure 2).

Annexure 2

Independent Samples Test

		Levene's Test		t-test for Equality of Means	
		F	Sig.	t	Sig. (2-tailed)
PER. UTL.	Equal variances assumed	3.043	.086	.000	1.000
	Equal variances not assumed			.000	1.000

Table 5: Mobile banking users vs. non-users

Issues	F	Sig. (p<0.05)
Mobile handset operability	0.789	0.378
Security/Privacy	3.313	0.073
Standardization	0.224	0.637
Downloading & Installing application software	0.015	0.902
Customization	0.020	0.888
Telecom Service Quality	0.753	0.389

8.6 Mobile banking perceived utility in comparison To other channels:

Overall users vs. non-users
Percentile analysis (Annexure 3) suggest that majority of the respondents (53.6%) were indifferent towards perceived utility of mobile banking in comparison to retail banking and internet banking.

Further an Independent Samples T-test was conducted to explore perceived utility of mobile banking in comparison to retail banking and internet banking students of users and non-users. There was absolute no significant difference in perceived utility between users (M=2.55, SD=0.83) and non-users (M=2.55, SD=1.03; t= 0.000, p= 1.000).

Annexure 3

PER. UTL.

		Output	Percent
Valid	100	1	10.6
Missing	0	2	12.4
		3	53.6
		4	15.2
		5	8.2
		Total	100.0

9. RECOMMENDATIONS

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 (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.

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 members 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 sub-committees 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. Al-Ashban, A.A. and Burney, M.A. **Customer adoption of tele-banking technology: the case of Saudi Arabia**, *International Journal of Bank Marketing,* 19 (5), pp. 191-200,2001.

2. Amir Herzberg. **Payments And Banking With Mobile Personal Devices**, Communications of the ACM, Vol. 46, No. 5, May 2003.

3. Banzal S. **Mobile Banking & M–Commerce and Related issues**, *www.* public.webfoundation.org/…..... / 25, Mobile_banking_M-commerce_15.03.pdf, 2010.

4. Barnes,S.J., and Corbitt, B. **Mobile Banking: Concept and Potential**, International Journal of Mobile Communications, 1 (3), pp. 273-288, 2003.

5. Black, N. J., Lockett, A., Ennew, C., Winklhofer, H. and McKechnie, S. **Modeling consumer choice of distribution channels: An illustration from financial services**, International Journal of Bank Marketing, 20(4), pp.161- 173, 2002.

6. C. Narendiran, S. Albert Rabara, and N. Rajendran. **Public key infrastructure for mobile banking security**, Global Mobile Congress 2009, pp. 1-6,2009.

7. 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.

8. Comninos, A., Esselaar, S., Ndiwalana, A. and Stork, C. **Towards evidence-based ICT policy and regulation mobile banking the unbanked**, http:// externo.casafrica.es/aeo/pdf/english / overview_part_2_09_aeo_09.pdf , 2008.

9. 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.

10. Dian Yan Liou. **Four‑scenario analysis for mobile banking development contextualized to Taiwan**, Management of Engineering & Technology, PICMET, pp. 2634-2642, 2008.

11. 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.

12. H. Harb, H. Farahat, and M. Ezz. **SecureSMSPay: Secure SMS Mobile Payment model**, Anti - counterfeiting, Security and Identification ASID, pp. 11- 17,2008.

13. 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.

14. Hayat Muhammad Aslam. **Mobile payments: Will Colombo keep its leadership in South Asia?**, http://sundaytimes.lk/090712/FinancialTimes/ft323.html, 2009.

15. I. Brown, Z. Cajee, D. Davies, and S. Stroebel. **Cell phone banking: predictors of adoption in South Africa--an exploratory study**, International Journal of Information Management,Vol.23, pp. 381-394, Oct.2003.

16. Jin Nie   and   Xianling   Hu. M**obile   Banking Information Security and Protection Methods**, Computer   Science and   Software Engineering, 2008 International Conference , pp. 587-590, 2008.

17. Karjaluoto,   H.,   Mattila,   M. and Pento, T. **Factors   underlying   attitude   formation   towards online banking in Finland**, International Journal of Bank Marketing, 20 (6), 261-272, 2002.

18. Lyman, T.R., Pickens M. & Porteous D., "Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance", *In: Focus Note 43*. Consultative Group to Assist the Poor (CGAP), Washington, DC, 2008.

19. Mas, I., "Realizing the Potential of Branchless Banking: Challenges Ahead", *In: Focus Note 50*. Consultancy Group to Assist the Poor (CGAP), Washington, D.C., 2008.

20. Mobile   Payment   Forum   of   India   (MPFI) http://www.mpf.org.in/

21. Muhammad Bilal, Ganesh Sankar, "Trust & Security issues in Mobile banking and its effect on Customers, School of Computing, Blekinge Institute of Technology, SE-371 79 Karlskrona Sweden, 2011.

22. P. Soni,─ M-Payment Between Banks Using SMS [Point of View], ‖ *Proceedings of the IEEE*, vol. 98, pp. 903-905. 2010.

23. Polatoglu, V.N. & Ekin, S., "An empirical investigation of the Turkish consumers' acceptance of Internet banking services", *International Journal of Bank Marketing*, 19 (4), 156-165, 2001.

24. Prerna Sharma Bamoriya & Preeti Singh, "Issues & Challenges in Mobile Banking in India: A Customers' Perspective", Research Journal of Finance & Accounting,Vol.2,No.2, 2011.

25. R. Fisher,─Business aspects of trusted third party services in Europe,‖ *Information Technology Applications in Biomedicine,   IT IS - ITAB ' 99. IEEE EMBS International Conference on*, pp. 38-39, 1999.

26. Rao, G. R. & Prathima, K., "Online banking in India", Mondaq Business Briefing, 11 April 2003. Sharma, Prerna & Singh, Preeti, "Users' perception about mobile banking- with special reference to Indore & around", *Review of Business & Technology Research*, Vol. 2, 1, pp. 1-5, 2009.

27. S. Alam, H. Kabir,   M. Sakib, A. Sazzad, C. Shahnaz, and S. Fattah, ─ A secured electronic transaction scheme for mobile banking Bangladesh incorporating digital   watermarking, ‖ *Information   Theory   and Information Security (ICITIS), 2010 IEEE International Conference on*, pp. 98-102, 2010.

28. S. Hung,C. Ku, and C. Chang, ─Critical factors of WAP services adoption: an empirical study, ‖ *Electronic Commerce Research and Applications*, vol. 2, Spring. pp. 42-60, 2003.

29. S. Wijetunge, P. Wijesinghe,   and   U. Gunawardana, ─ Social Impact of SMS in Sri Lanka,‖ *Information and Automation for Sustainability, 2008. ICIAFS 2008. 4th nternational Conference on*, pp. 346-350, 2008.

30. Suoranta, M., "Adoption of mobile banking in Finland", *Jyväskylä Studies in Business and Economics*, 28, 2003.

31. Suraj - sankaran, "Mobile Banking   Architecture :Palisade", http://palisade.plynt.com / issues /2007May / mobile-banking / ,MAY, 2007.

32. T. Holz, M.Engelberth,   F. Freiling," Learning   More about the Underground Economy", ESORICS 2009, LNCS 5789, pp. 1–18, 2009

33. T. Wilson, ─ Malicious   mobile   ode, ‖ *Internet Business*, pp. 52-3, Feb.1999.

34. Unithan, C. R. & Swatman, P.,   "Online banking Adaptation and Dot.Com Viability: A Comparison of Australian and Indian Experiences in the Banking Sector", School of Management Information Systems, Deakin University, No. 14, 2001.

35. Xiaoping Zhang and Cheng Zhong, ─A Loss Reportable E - Cash Scheme without TTP Based on ECC, ‖ *Management of   e-Commerce   and e-Governmen, ICMECG '08. International Conference on*, 2008, pp. 354-358, 2008.