Chapter 1

Introduction
This chapter examines the background of the research, problem statement and research objectives of the research. It also highlights the limitations and delimitations of the research.

INTRODUCTION

The world is coming closer with rapid development of Information and communication technology, one such technological wave which is spreading all over the world is increasing usage of Cell Phone (Mobile Phones) for various activities.

A cell phone user uses cell phone not only for making calls but a lot more than that. Mobile Phone is getting popular among Banks and Users as a tool for making financial transactions.

Uses of making cell phone for financial transaction know as mobile banking. The concept of mobile banking gives flexibility to do banking transaction like fund transfer, balance enquiry, etc. These transaction not only restrict to full fill banking needs but also selling and purchasing goods by doing fund transfer to merchant using third party software. Easy accessibility and 24 by 7 availability attracts mobile uses and so increases in uses of mobile. As uses of mobile increases there is increase in use of banking operations over cell phone.

The myth follows with mobile banking is that financial transaction can done through websites and mobile application over internet such as SBI Freedom, Star Connect etc but the fact is that mobile banking can be done in offline mode as well by using SMS Banking, M- Wallets etc.

A new wave of mobile technology solutions, including mobile banking apps that turn any smartphone into a fully operational personal bank, is sweeping through the banking industry. With cash transfers between mobile phones increasingly becoming a reality, mobile banking could soon become as commonplace as Internet banking (source: ...
Banking
As Indian and other countries uses paper currency as a medium of fulfilling daily needs there is need to have a medium to safe guard the paper currency. The bank provides an medium to provide the safe guardness to the paper currency and may provide several alternatives to fill the daily needs of human being. Those medium called as banking.

Banking is the financial organization which used to keep money not only to safe guard but also providing profits to the customer as well as to serve customer by providing various options to use the money for various transactions. As time passes away the banks adopts new technologies for financial transactions instead of traditional banking practices. Such as use of ATM instead of token system, use of SMS Banking for balance enquiry and tablet banking for opening the bank account etc.

The banking sector's first ATM debuted in the late sixties, nearly five-and-a-half centuries after the world's first modern bank. From there, the pace of automated customer interfaces really stepped up - online banking in the mid-nineties, mobile banking in the early aught and social media access in 2012.

A sharp increase in use of smartphones has led to a sudden surge in mobile banking transactions — almost four times in a year in value terms.

Financial Transaction: Currency involved transaction known as financial transaction. The transaction can between two persons, two organizations etc.
Trust is important parameter while performing financial transaction even if someone provides trust along with profit then there is well and good for consumer. The bank provide same to consumer so generally financial transaction will be take place by keeping bank as third party vendor.
As time progresses the ways of doing financial transaction also become advanced from 4C payment methods (Cash, Cheque, Credit and Credit/Debit) to E-banking and in today’s era up to mobile banking.

**Mobile Banking**
Mobile is a device with users connected more. A device which user carries almost 24 by 7 with them for doing various activities such as phone calls, Sending or receiving SMS / MMS etc. but in today’s information era mobile phones not just used for making phone calls but also use for various activities such as to access the internet, making information available on figure tip etc. The use of internet increases the application of mobile phones and because of that the cell phone can be used as median to do financial transactions. The financial transaction done though cell phone known as Mobile Banking. Mobile banking is an alternate channel for providing banking services. India is the second largest country which has telecom market in the world which is having high potential for expanding banking services using mobile phones. Mobile banking is making finance related functions on a mobile device like a Smartphone or tablet. According to TRAI, mobile banking involves the use of mobile phones for banking transactions like fund transfer, balance check, etc.

Hence Mobile banking services can be broadly classified into

**SMS Banking**
SMS Banking is a service that allows customers to access their account information via mobile phone. SMS banking services are operated using both push and pull messages. Push messages are those that the bank chooses to send out to a customer's mobile phone, without the customer initiating a request for the information. Pull messages are those that are initiated by the customer, using a mobile phone, for obtaining information or performing a transaction in the bank account.

**Application (Software) Oriented**
A *mobile-optimized website* is a website that is intended to be viewed using a mobile browser on the various display sizes of phones, tablets, and other mobile devices. Mobile
websites are typically simplified versions of a standard website that provide a better mobile user experience through improved usability, faster page loads, and sometimes reorganization of content to bring mobile-specific features to the forefront of the experience.

**Mobile Application**

Also called mobile apps, it is a term used to describe Internet applications that run on smartphones and other mobile devices. Mobile applications usually help users by connecting them to Internet services more commonly accessed on desktop or notebook computers, or help them by making it easier to use the Internet on their portable devices. A mobile app may be a mobile Web site bookmarking utility, a mobile-based instant messaging client, Gmail for mobile, and many other applications.

**M- Wallet**

Mobile wallets, allows non-banking customers to open a bank account (with minimum KYC documents) and avail range of financial services in addition to utility services and merchant payments. The advantage of mobile wallet is secure storage of money and any-time, any-where usage of the wallet to avail range of services and make payments. The future of payments is mobile wallet. It can empower non-banking stream customers with the essential access to banking, payments and other services.

Looking at the above facilities provided it is evident that Banks are now increasingly choosing mobile platforms for innovative payment models and commerce capabilities, but all these mobile banking services comes with some security risks.

The technology used must be secure and at the same time convenient to deploy and cost effective. The following technology basis provides a summary of the available models. Banks must deploy only secure channels that provide a non-repudiable platform to transact.
<table>
<thead>
<tr>
<th>Telecom Standard</th>
<th>Data Bearer</th>
<th>User Interface</th>
<th>Method of Invoking / Initiating Transactions</th>
<th>Security</th>
<th>Hardware / Setup Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSM</td>
<td>Plain Text SMS</td>
<td>Structured Text</td>
<td>SMS / J2ME</td>
<td>Weak Encryption</td>
<td>Works on any phone. Workarounds like IVR call backs for sensitive information are possible</td>
</tr>
<tr>
<td>GSM</td>
<td>USSD / Application SMS</td>
<td>GUI (Graphic User Interface) / Structured Text</td>
<td>SMS / J2ME</td>
<td>Secure Channel</td>
<td>J2ME client requires Java enabled phone.</td>
</tr>
<tr>
<td>GSM</td>
<td>GPRS / WAP</td>
<td>GUI</td>
<td>J2ME / Browser</td>
<td>Secure Channel</td>
<td>Java enabled phone with GPRS. Without GPRS this can work within the Telecom provider’s walled garden.</td>
</tr>
<tr>
<td>CDMA</td>
<td>Application SMS / GPRS / WAP</td>
<td>GUI</td>
<td>Brew / Browser</td>
<td>Secure Channel</td>
<td>Operator centric usage</td>
</tr>
</tbody>
</table>

**Table 1.1 Summary of technology used for mobile application development**

In order to ensure a level playing field and considering that the technology is relatively new, Reserve Bank has brought out a set of operating guidelines for adoption by banks.
The overall security framework should ensure.

- Encrypted messaging / session between consumer’s phone and third party service provider / Telecom Company. Minimum encryption standards to be specified to make the transaction banking grade (E.g. Min 128 bit SSL)

- All subsequent routing of messages to the bank’s servers must be with the highest level of security with dedicated connectivity like leased lines / VPNs.

- If any sensitive information is stored in third party systems, banks must ensure that access to this information is restricted with appropriate encryption and hardware security standards.

- All transactions that affect an account (those that result in to an account being debited or credited, including scheduling of such activity) should be allowed only after authentication of the mobile number and the mPIN associated with it. Transactions only for information such as balance enquiry, mini statements, registered payee details, etc may be allowed with either mobile number or PIN.

- Unless fool proof security is used in compiling and deploying the mobile banking applications, the PIN number should not be allowed to be stored in the mobile banking application on the phone. As, generally the application installed on the phone would be developed in Java, it may be possible to decompile it extract the mPIN. Alternatively, the application should be so compiled that it should not be feasible to extract the PIN on decompilation.

- All accounts, credit or debit cards allowed to be transacted through the mobile phones should have the mobile phone number linked to the account, credit or debit card. This mobile number should be used as the second factor authentication
for mobile transactions.

- During the transaction, the PIN should not travel in plain text. Doing this, there is risk of the PIN being snooped out of the phone from sent items and also it being exposed at the SMSC level. Also, it may be able to snoop out the PIN during transmission, although, this is very difficult in cellular communications.

- Proper level of encryption should be implemented for communicating from the mobile handset to the mobile payments service provider’s server. It has been assumed that proper security checks would be made by the banks to ascertain the security levels of the service providers. This may include PCI DSS certification in addition to bank’s own audits.

- Proper system of verification of the phone number should be implemented, wherever possible. This is so as to guard against spoofing of the phone numbers as mobile phones would be used as the second factor authentication.

- It is also recommended that Internet Banking login ids and passwords may not be allowed to be used through the mobile phones. As fraudsters get more sophisticated, the chances of phishing attacks on mobile phones would become more probable. Allowing Internet banking login id and password usage on the mobile phone may compromise their usage on the Internet banking channel. This restriction may be communicated to the customers through an industry wide effort so as to ensure that Internet banking passwords are not compromised through mobile phones.

- The payment authorization message from the user’s mobile phone should be securely encrypted and checked for tampering by the service provider or the bank. It should not be possible for any interceptor to change the contents of the message.
• Provided the above security recommendations are reviewed, the mobile payment service could use any of the preferred modes of communication viz., SMS, IVRS, WAP/GPRS, USSD and NFC. There are couple of security issues in some of these modes of communications, which are listed below:

  a. SMS is the simplest form of communication, but is vulnerable to tampering. As long as there is a second level of check on the details of the transaction so as to guard against data tampering and the mPIN does not travel in plain text, this mode of communication can be used.

  b. IVRS is also a simple mode of communication and therefore does not have any inbuilt security measures. The system should be capable of encrypting the DTMF tone entries, if required to be stored or transmitted.

  c. USSD communication uses its inbuilt encryption technology to talk between the cell phone and the operator’s server. However, the decryption of the information happens at the cell phone operator’s server. Vulnerability of data may exists at this point. This information should be re-encrypted and transmitted to the service provider.

• Any of the following modes of user interface may be used, provided the above listed security measures are taken into consideration:

  a. SMS  
b. Menu driven application  
c. Menu driven USSD application  
d. WAP/GPRS website

• Formats need to be specified for exchange of information between banks. On the debit/credit card front, the exiting ISO 8583 message format may be used for communication between bank switches. However, for account number based
mobile transfers, a message format may need to be frozen.

- Banks should designate a network and database administrator with clearly defined roles as indicated in the technology Group’s report

- Banks should have a security policy duly approved by the Board of Directors. There should be a segregation of duty of Security Officer / Group dealing exclusively with information systems security and Information Technology Division which actually implements the computer systems. Further, Information Systems Auditor will audit the information systems.

- Banks should introduce logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. Logical access control techniques may include user-ids, passwords, smart cards or other biometric technologies

- At the minimum, banks should use the proxy server type of firewall so that there is no direct connection between the Internet and the bank’s system. It facilitates a high level of control and in-depth monitoring using logging and auditing tools. For sensitive systems, a stateful inspection firewall is recommended which thoroughly inspects all packets of information, and past and present transactions are compared. These generally include a real time security alert.

- All the systems supporting dial up services through modem on the same LAN as the application server should be isolated to prevent intrusions into the network as this may bypass the proxy server.

- The information security officer and the information system auditor should undertake periodic penetration tests of the system, which should include:
- Attempting to guess passwords using password-cracking tools.
- Search for back door traps in the programs.
- Attempt to overload the system using DDoS (Distributed Denial of Service) & DoS (Denial of Service) attacks.
- Check if commonly known holes in the software, especially the browser and the e-mail software exist.
- The penetration testing may also be carried out by engaging outside experts (often called ‘Ethical Hackers’)

- Physical access controls should be strictly enforced. Physical security should cover all the information systems and sites where they are housed, both against internal and external threats.

- Banks should have proper infrastructure and schedules for backing up data. The backed-up data should be periodically tested to ensure recovery without loss of transactions in a time frame as given out in the bank’s security policy. Business continuity should be ensured by setting up disaster recovery sites. These facilities should also be tested periodically

**CHALLENGES WITH ADOPTION OF MOBILE BANKING**

1. **Financial Challenge**: India is spread across 600,000 villages, each with a low transaction value. India is farmer’s country and most of the people in India are below poverty line. Most of the people still didn’t offer to have Smartphones with high speed internet connection.

2. **Literacy**: India spread across 600,000 villages and most of the people are illiterate so it’s difficult them to access internet over cell phone even doing financial transaction over cell phone

3. **Regulatory Challenges**: Although the RBI is supportive of mobile banking in India, there are many regulations that are being put into place
4. **Y-Generation**: India is the country which has 60% population between age group 20-50 Years. This generation requires always new things. So its big deal with application developers to keep youth connected with technology by doing continuous improvement.

5. **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.

**Problem Statement**
In today’s era every individual requires technology to full fill daily needs not only to connect with each other but also for doing financial transaction such as buying and selling goods, fund transfer etc almost for every activity we have to depend on technology. This technology has been equipped with devices even small in size day by day from mainframe computer to Personal Computer even laptop and smart phone. The smart phone equipped with latest APP’s can be used for making daily financial transaction but smart phone user’s has few myth’s such as security, confidentiality etc but as per developers opinion financial application are secure as secure manual transaction. The problem has been started by keeping user’s myth’s in mind. The important factor of study is security of financial transaction done through smart phone. The researchers has to study that whether the financial transaction applied via cell phone are secure if no then finding the security measure for making transaction secure.

**Status of Mobile Phones in India**
TRAI was set up in the year 1997 for the regulation of telecommunication sector in India. In March 1999 National Telecom Policy (NTP) was announced. In 2003 CDMA network was launched. In 2004 Broadband policy was announced. Mobile phone subscribers had reached 100 Million by 2006. In 2008, RBI issued operative guidelines for banks for mobile banking transactions in India. By the year 2009, wireless subscriber base crossed 400 million. At present wireless mobile phone subscribers are 867 Million i.e. it has almost doubled in the last four years.
According to report of TRAI and COAI Maharashtra has added 8.7 lakh subscribers in December 2014 in rural India. This figure is maximum among all circle. Karnataka, Kerala and Rajasthan have 5.4 lakh, 5.1 lakh and 4.2 lakh subscribers in December 2014 in rural India.
Looking at above statistics we can say that Mobile phone is a common technology device that became part of every individual in the information era which can be confirmed by another report by TRAI that says subscribers who access the internet through wireless phones are approximate 143.2 Million(2014).

Due to this tremendous growth of the mobile phone industry most financial institutions have ventured into the untapped opportunity and have partnered with mobile phone network providers to offer banking services to their clients.

Mobile payment is enabled by a variety of emerging technologies, many of which are still maturing (Eze et al., 2008). These technologies are needed to address various payment industry needs which includes secure authentication infrastructure on mobile devices, secure transmission infrastructure for wireless payment, trust/validation directories and virtual “wallets” stored on a mobile device or accessible over a network (Taga et al., 2004).

Despite all the technological advancement in mobile technology, security is still an important issue with financial transaction through Mobile Banking. Basic phones with mobile money capability could be described as GSM (Global System for Mobile) compatible phones with embedded services such as SMS and USSD (World Bank, 2012). There is however, no end-to-end security for SMS, protection ends in the GSM or UMTS (Universal Mobile Telecommunications System) network. Furthermore, unstructured supplementary service data (USSD), has no separate security properties; instead it relies on the GSM/UMTS signalling plane security mechanism (just like SMS). It is further argued that the security mechanisms of authentication, message integrity, replay detection and sequence integrity, proof of receipt and proof of execution, message confidentiality and indication of security mechanisms exists; however, it depends on the applications
whether these security mechanisms are implemented and whether their cryptographic strength is sufficient (Schwiderski-Grosche & Knospe, 2002).

As per the extant guidelines of RBI, banks that are licensed, supervised and have a physical presence in India, are permitted to offer mobile banking services. Mobile Banking policies in India aim to enable funds transfer from an account in any bank to any other account in the same or any other bank (interoperability) on a real time basis irrespective of the mobile network the customer has subscribed to (TRAI, 2013). The Mobile phone plays a very important role in the development of mobile commerce and mobile banking.

Also there is Massive and steady Growth in Mobile users in Maharashtra State. However, mobile banking has not become the choice of people. The main objective of this study is to identify and analyze the security issues in Mobile banking among the banking customers and the preventive measures undertaken by developers of such system. Hence the problem statement Financial Transaction through Cell Phone a Critical Analysis of Security Risk and Preventive Mechanism

**Limitations:-**

It is purely a study of user’s of cell phone who use cell phone for financial transaction and developers of smart phone application.

The population in respect of users is any user who uses cell phone for financial transaction. The sample of users is collected from urban and rural area by region

The developers are the developers who create smart phone application used for banking purpose
References

• Lee, YS, Kim, E & Jung, MS 2013, “A NFC based Authentication method for
defence of the Man in the Middle Attack” 3rd International Conference on
Computer Science and Information Technology (ICCSIT’2013) January 4-5, 2013
Bali, Indonesia.
• Schwiderski-Grosche, S & Knospe, H 2002, Secure M-Commerce, Information
Security Group, Royal Holloway University of London, Egham TW20 0EX, UK.
• Taga, K, Karlsson, J & Arthur, D 2004, Little Global M-Payment Report, Austria,
Vienna.

• http://www.coai.com/
• http://www.trai.gov.in/
• http://www.slideshare.net/amarjeetbains1/online-banking-challengesandopportunities
• http://www.banknetindia.com/banking/ibguide1.htm
• https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1365
• http://www.wipro.com/blogs/smart-money-how-mobile-technology-is-
transforming-the-banking-industry/
• http://mindinmotion2010.tumblr.com/post/112296414408/banking-related-
mobile-apps-know-how
• http://www.techcusp.com/blog/mobile-applications-for-banking-a-smart-way-to-
provide-services-by-techcusp-com/
• http://mimgroup2010.blogspot.in/2015_02_01_archive.html
• http://iqipixe.boxhost.me/sujihe/hewylefo.html