

Determining New Security Challenges for Mobile Banking

Dr. Syed Nisar Osman
Dept. Of Computer Science
Lal Bahadur Shastri College Dhamabad Dist. Nanded [MS]
dr.nisar73@gmail.com

Abstract: Technology plays an important role in banking sector. Banking is one of the largest financial institutions constantly explores the opportunity of technology enabled services to provide better customer experience and convenience [1]. Mobile phone is a common technology device that became part of every individual in the information era. Mobile Banking is an emerging alternate channel for providing banking services. India is the second largest telecom market in the world, which is having high potential for expanding banking services using mobile. However, mobile banking has not become the choice of millions of people. The main objective of this study is to identify the mindset and analyze the security issues in Mobile banking among the banking customers in India

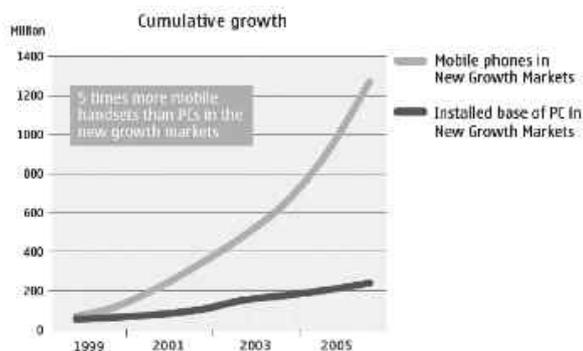
Keywords – Mobile Banking, Net Banking in India, Security Challenges.

1. INTRODUCTION

The main advantage of Mobile Banking is that the people in remote area can also access the banking services at ease[1]. This has become possible with the reach of mobile devices in the rural areas where the device can be purchased starting from few hundreds.

The penetration of mobile in India has made rapid change in communication system. Apart from the reach of communication device; revolution in mobile technology like 2G, 3G, and 4G are created more market where the potential people are adopting the latest technologies. One is communication and connectivity and other is business process. Today, banks have welcomed wireless and mobile technology into their boardroom to offer their customers the freedom to pay bills, planning payments while stuck in traffic jams, to receive updates on the various marketing efforts while present at a party to provide more personal and intimate relationships Many believe that mobile users have just started to fully utilize the data capabilities in their mobile phones. In Asian countries like India, China, Indonesia and Philippines, where mobile infrastructure is comparatively better than the fixed-line infrastructure, and in European countries, where mobile phone penetration is very high (at least 80 per cent of consumers use a mobile phone), mobile banking is likely to appeal even more. This opens up huge markets for financial institutions interested in offering

value added services. With mobile technology, banks can offer a wide range of services to their customers such as doing funds transfer while traveling, receiving online updates of stock price or even performing stock trading while being stuck in traffic. According to the German mobile operator Mobilcom, mobile banking will be the "killer application" for the next generation of mobile technology.



2. Application of Mobile Banking

- **Mobile Banking:** Enabling users to perform banking transactions using mobile phone like, balance checks, fund transfers, bill payments, etc.
- **Remote Purchase:** Using the mobile phone to purchase goods over the internet or for home delivery. For e.g. paying for a dominos pizza from home
- **Person to Person Transfers:** Using mobile phones for remittance transfers.

- Point of Sale: Using phones to pay for goods at merchant location

3. MODE OF SERVICES

SMS: Most of the popular services are currently based on SMS. These services use the following process flow:

1. Customer sends an SMS initiating payment. As part of the SMS customer enters the pin number, amount and recipient's unique identification number (can be mobile text fonts are prescribed; please do not alter them. You may note peculiarities. number of account number)
2. There is a acknowledge cycle for every SMS and Transactions can span over multiple SMSs USSD (Unstructured Supplementary Service Data): Some services have been built utilizing USSD technologies. USSD messages are initiated by dialing short codes. For e.g. *#111#123456#. Process flow followed is similar to above. GPRS / CDMA: GPRS / CDMA describe services based on mobile internet. These are more advanced services and can allow users with variety of features to conduct transactions. Typical usage scenario is described below:

1. Customer visits a website using his phone and initiative transaction using pin number and phone number as a combination
2. Alternatively the customer can open an application residing on this phone and initiative payment by selecting merchant / product.
3. All data communication is over the internet protocol and following normal e-commerce based practices

4. SERVICES OFFERED THROUGH MOBILE BANKING

- a. Account Information
- b. Payments & Transfers
- c. Investments
- d. Content Services

5. SECURITY CHALLENGES

The following aspects need to be addressed to offer a secure infrastructure for financial transaction over wireless network [8]:

1. Physical security of the hand-held device. If the bank is offering smart-card based security, the physical security of the device is more important.
2. Security of the thick-client application running on the device. In case the device is stolen, the hacker should require ID/Password to access the application.
3. Authentication of the device with service provider before initiating a transaction. This would ensure that

Unauthorized devices are not connected to perform financial transactions [11].

4. User ID / password authentication of bank's customer.
5. Encryption of the data being transmitted over the air.
6. Encryption of the data that will be stored in device for later / off-line analysis by the customer.
7. All messages originating from your mobile phone are encrypted and travel to our Mobile Banking Server in secured mode. The encryption methodology used in 128 bit AES technology. In the WAP based service, the site is VeriSign certified.
8. memories your User ID and delete SMS containing the information
9. After receiving the SMS with User ID and default MPIN, immediately log on to Mobile Banking and change your default M-PIN
10. Don't disclose your User ID to anyone
11. change your MPIN at regular intervals
12. Don't use obvious passwords (like name, date of birth, etc.).

6. CONCLUSION

The aim of work is to focus on mobile banking to analyze the different factors as Negative and Positive that impact adoption of mobile banking, and to introduce the mobile banking emerging technologies and services. It is well recognized that mobile phones have immense potential of conducting financial transactions and there are many positive factors are introduced such like Time Saving, Reduction of obstacle to move physically one place to another , To Control Fraud, Easy to avail Mobile Services and Reminder Facilities and have some Negative Factors are also introduced like Security.

Acknowledgement

We are thankful to them who have co operated me directly and indirectly with support at all times for this project.

REFERENCES

- [1] Sharma, Prerna, Bamoriya & Preeti Singh (2011) - Issues & Challenges in Mobile Banking In India: A Customers' Perspective
- [2] www.bankrate.com/finance/banking/finding-best-mobile-banking.aspx
- [3] <http://www.thejakartapost.com/news/2012/05/11/commonwealth-bank-tapping-growing-mobile-banking-market.html>
- [4] www.palgrave-journals.com/jbr/journal/v11/n2/abs/jbr200916a.html
- [5] <http://warse.org/pdfs/ijatcse03122012.pdf>
- [6] <http://www.trai.gov.in>
- [7] <http://www.rbi.org.in>

[8] <http://www.sbi.co.in>

[9] <http://en.wikipedia.org>

[10] www.iiste.org

[11] http://www.trai.gov.in/WriteReadData/WhatsNew/Documents/Monthly_press_release_February_2013_16april2013.pdf

[12] <http://www.newfreeppt.com/banking/mobile-banking-ppt-free-download>

[13] Pandey, Atul 2012. Study Material on Electronic Banking and Electronic Payment Systems, NLIU, Bhopal