Customers Perception on Security System in Mobile banking

***P.Sailaja**
****Dr.V.Thamodaran**

*** & **** PhD Research Scholar and Assistant Professor, Dept. of Business Administration
Annamalai University, Chidambaram, India

Abstract

The emergence of E-Banking (Electronic Banking) changed the entire revolutionary concept thereby increased the usage widely leading to more innovation, development in banking technology. In which one of the major development in combination of E-commerce and E-banking technology is Mobile, SMS and Phone banking. Wherein the customers can view their account details, banking transactions, payment of bills, payment of credit cards, transfer of funds, obtain financial products or services information or applying/renewing like fixed and recurring deposits etc by using Mobile banking, SMS and Phone banking. This helps the customers can perform banking activities and its services on the move. The other major E-Banking services are ATM, internet/online banking, Net banking, Mobile banking, SMS banking and Phone banking. This paper has dealt with customers' satisfaction towards security system in EDC as part of e-banking and its preventive measures.

Keyword: Security system in Mobile banking or SMS banking or Phone banking.

I. Introduction

1.1 Concept of E-Banking

Due to advancement in Internet, WWW , Mobile Technology, Smart phones and E-Commerce many innovations started craving and implemented keeping a motto to ways to make it electronically digitized for easy operations at your fingertips for users, business, government, banks etc. Based on which one of the biggest breakthrough and presently used at a large scale all over the world is E-Banking i.e. Electronic Banking. The emergence of E-Banking changed the entire revolutionary concept thereby increased in usage widely and thereby more innovation, development and increase in online shopping, e-commerce, e-payment and banking.

E-Banking is where banking is done electronically through various technology and devices like ATM (Automated teller Machine), Online/Internet Banking / Net banking, E-Payment, Mobile banking, Phone banking, SMS banking, Swiping at vendor outlet etc by using debit and credit card, A/C no., customer number, customer User ID, Password, Authentication codes, OTP Pin, ATM Pin no. etc.

This enables the financial institutions, individuals or businesses, to access accounts, transact business and apply or obtain information on financial products and services which can be performed electronically i.e. via internet etc. Due to emergence of E-Banking it saved customers in avoiding long queue, transport, cost delays and thereby creating an environment of trust between the bank and customer for more faster, reliable, efficient and personalized services. Banks through internet has emerged as a strategic resource for achieving higher efficiency.

1.2 Evolution of E-Banking

Earlier traditional banking industry deals with few schemes like savings, deposits, loans etc. and also for the bank it is a manual tedious process of maintaing and tracking the accounts and transaction of each and every customer. Even customers equally had the difficulties of coming to the banks, long queue system, sometimes no proper response from the banks, need to come repetitive times to the bank for any banking transaction or information, lack of benefits and infrastructure for customers, lack of different types of schemes and banking services.

Due to emergence of computer (1950), E-Commerce (1972) and worldwide web (1989) carved in development and innovation of E-Banking (started in 1970 and strategic imperative in 1990), ATM (1967-2000) , SMS banking (1980) and Mobile banking (2010). Due to the emergence of E-banking changed the entire revolutionary thereby leading to increase in usage widely and more innovative development in E-commerce, E-payment and banking sector etc. In this modern banking the storage space is reduced, and 24/7*365 days banking from anywhere in the world and banking services/customer care support round the clock thus making modern banking or the emergence of E-banking system user friendly and cost effective system.

1.3 Mobile Banking, SMS Banking and Phone Banking

Due to the advancement of Smart phones especially android, mobile banking apps of the respective banks are installed in the smart phones wherein the customers can perform banking activities on the move. Mobile banking activities like the customers can view their account details, banking transactions, payment of bills, payment of credit cards and transfer of funds, obtain financial products or services information or applying/renewing like Fixed deposit or recurring deposit etc.

To view the instant banking account transaction or details, account balances, information, Fund transfer, PIN Change, OTP PIN authentication message, banking activities like stop payment etc via mobile SMS it can be either via request sent by SMS or from bank auto generated SMS.

Phone banking is doing banking transactions and for attaining banking related information or services which are done by calling the registered phone banking no. provided by the bank by which the customers can perform the banking transactions by IVR or via customer care support person. Now currently even customer support via video interaction facility is also being launched by Indusland bank in India via mobile app.

This has helped in getting up to date information/updates and doing transactions on the move without visiting the bank and thereby reducing cost, transport, visit to the bank etc. This has lead to the bonding relation between the bank and the customer and rarely visiting to the bank. Also simultaneously banks are also improving on customer support and its services and thereby developing more apps, application, door step services, information/services via phone banking IVR etc.

But on the contrary there is a rise in cyber crime frauds/threats/hoax calls and other criminal activities and few of the fraudster making it professional too leading to not only stealing sensitive information but also banking related information especially bank credentials, reading the SMS received and emails, sending mails or making calls and erasing the data without the knowledge of the customers. By the time the customers realize huge amount of money will be missing from bank account, sensitive information is stolen, phone balance is nil, hoax mails and SMS at lot, data loss, virus attack corrupting the phone and making the phone dead.

Based on investigation by cyber crime police it is found that these kinds of attacks are done by youngster and teenagers for the sake of fun or use to say for learning purpose but there are also others who do it real time and professional just to make easy money. All of these fraudsters/criminals attack either via hoax calls for gathering card details and CVV no. etc or else sending virus via email/SMS thereby hacking the mobile especially smart phones etc causing a threat for the customers and sometimes reputation of the Banks and law enforcement is being effected for protection against these crimes.

Customer Awareness and Education on security Measures for Secured Mobile, SMS and Phone banking:

Customer and vendor education and awareness are one of the important tools to ensure secured electronic banking. Following are some of the measures undertaken by banks in this regard:

- To change Password periodically ensure separate strong password for login and transaction

- Install anti-virus software and firewall on your mobile handset to protect against viruses and ensure it is up-to-date.
- Download and run security updates and patches on your mobile browser. This helps in protection from known possible security problems.
- Remove all the temporary internet files after using mobile banking services.
- Delete the browsing history of your mobile browser on a regular basis.
- Do not open attachments or links from unknown sources. This helps in protection from viruses or other unwanted problems.
- Type in the URL for mobile banking in the mobile browser, instead of clicking on any link. This will ensure access of the authentic website of the bank.
- Ensure that Mobile banking app is downloaded from relevant App Store. (Eg: PlayStore for Android OS)
- Update to latest version of Mobile banking app whenever it is available in relevant App store
- Act with caution while installing any third party software on your mobile handset to avoid spyware. Do not install pirated software or software from unknown sources.
- Delete spam messages.
- Be aware of the potential for fraudulent SMS messages. The Bank will never request or invite customers to logon to its mobile banking service via a SMS message.
- Check that the security padlock on your internet browser is "locked" to ensure the connection is secure and protected by SSL. You should also check that the URL starts from 'https' and not 'http'.
- Report a lost or stolen phone immediately to your service provider and law enforcement authorities
- Review your account statements frequently to check for any unauthorized transactions
- Be cautious while accepting offers such as caller tunes or dialer tunes or open/download emails or attachments from known or unknown sources
- Don't store sensitive information such as credit card details, mobile banking password and user ID in a separate folder on your phone
- Never reveal or write down PINs or retain any email or paper communication from the bank with regard to the PIN or password
- Be cautious while using Bluetooth in public places as someone may access your confidential data/information
- During phone banking - while speaking with the customer care person never disclose 4 digit ATM/IVR pin, OTP, net banking password, CVV, providing verification details in public places, and no one see the details especially PIN no. while entering, to complete self authentication
- Verify transaction details, OTP details etc received via SMS is secured and it is from the registered bank
- An SMS will be sent to you after completing any transaction. Please check transaction details carefully.
- To inform if any unforeseen cyber threat is noticed to the banks and if required to the Cyber-crime police

II. Review of Literature

Harshad Patel and Vijay Pithadia, (2013)[1] found that "Advancement achieved in the Information Technology and communication Technology in the last two decades has resulted in the successful implementation of Electronic Banking in India". Today, the banks able to offer the choice of customer services to provide banking business across the bank counter, over the telephone or through computer or internet. "The key to survival, therefore, is maintenance of customer loyalty by providing them with value added services customized to their needs. The focus of study is to certain the role of value added services to satisfy and retain customer loyal. Some of these value added services Automated Teller Machines cards (ATM), Credit card, Debit card, Internet banking, Tele banking, Mobile banking, Home Banking and so on.

Shumaila et.al (2003)[8] and N.B.Jadhav et. al (2011)[2] described E-Banking a method of banking in which customers conducts the transaction electronically via internet 24/7*365 days. It is widely used and due to the emergence of E-banking there is a drastic increase in E-commerce like online shopping, bill payment etc. Even the government and other private institutions and financial institutions are moving towards the internet and mobile world of technology and making it online and transparent. The reason behind going into online is because it is easy to track, search for information instantly, storage space is more, easy for analysis, interpretation of data thereby decision making and due to emergence of e-banking it helped in doing banking transaction, viewing account transaction, receiving transaction updates immediately, applying and using banking related products, fund transfers, profile update like change of phone/email id details etc instantly, track of other accounts, e-payment and bill payment etc by using PC or mobile devices. The different types of electronic banking are SMS banking, internet banking, Mobile banking, net banking, phone banking, ATM, e-payment etc. thereby giving convenience to customers to do banking transactions or view information or details etc anytime or anywhere. Electronic banking is the latest in the series of technology wonders in the recent past, involving use of internet for delivery of products and services. Banks through internet has emerged as a strategic resource for achieving higher efficiency. Due to emergence of E-banking it saved customers in avoiding long queue, transport, cost, delays etc. and thereby creating banks more faster and efficient and providing more personalized services to the user customer.

Tommi (2007)[3] explored and compared customer value perceptions in internet and mobile banking in Finland using a qualitative in-depth interviewing method. The means-end theory has been taken as the theoretical background for the study. According to this approach, the way the products and services relate to customers can be represented by three levels: attributes consequences and desired end-states. Attributes describe the product or service, consequences describe the benefits that the customer derives or seeks as a result of product or service consumption, the desired end states are seen as the ultimate ends that are served by the product or service means. The results indicate that efficiency, convenience and safety are the most important desired end-states of bank customers determining the differences in customer value perceptions between internet and mobile banking. It is found that the small screen of the mobile phone makes the device very difficult to use in fund transfer. The customers were found more worried about their own errors made while using the service rather than data security or other security issues.

Ravi et al, (2008)[4] stated that with the advent of innovative technology, banks were able to provide customized products and services like internet banking, mobile banking, ATMs, Tele - Banking, to their customers. Latest technology helped the banks to reduce their transaction cost. But certain risks associated with innovative technology and technology related frauds were found to increase. In order to provide smooth and safe banking to their customers, banks must enhance the technology related security.

Vanessa Pegueros (2012)[5] stated that mobile banking and payments in ecosystem is complex and dynamic and competition in the growing space from a financial services, application provider and technology perspective. Security and perception of security will clearly play a role ends up dominating. The wireless carriers are entering a segment with little financial service experience. Also wireless carriers and application providers are clear

disadvantage in understanding regulatory environment faced by current financial service providers.

Thakur and Srivastava (2013)[6] investigated the factors influencing the adoption intention of mobile commerce. For the study purpose research model was developed based on constructs from the technology acceptance model and innovation resistance theory. Perceived usefulness, perceived ease of use and social influence were found to be significant dimensions of technology adoption readiness to use mobile commerce while facilitating conditions were not found to be significant. The results also indicated perceived credibility risk defined by security risk and privacy risk was significantly associated with behavioural intention in negative relation, which indicated that security and privacy concerns are important in deterring customers from using mobile commerce.

III. Research Methodology and Analysis

1.1. Objective:

To analyze the factors that influences the security system of Mobile, SMS & Phone Banking a part of e-banking services and also to evaluate customers' satisfaction towards various factors of security system in e-banking services

1.2. Path Analysis

The above path analysis is run on a sample of 422 respondents to know the correlation and regression of independent variables with respect to satisfaction level regarding security on using Mobile, SMS & Phone banking. Likewise the independent variables are accessibility, security awareness, reliability, cost effectiveness, responsiveness, service quality and technical improvement and the second dependent variables or mediator variables are service factors on security and Technical factors on security Mobile, SMS & Phone banking.

1.3. Model Fit

Table I. Model Fit

Chi-Square	p	DF	RMS	RMSEA	GFI	AGFI	CFI	NFI
0.175	0.916	0.087	0.059	0.000	1.000	0.998	1.000	1.000

From the above table it is found that the calculated chi-square value is 0.175, p value is 0.916 which is greater than 0.05, which indicates perfectly fit. Here GFI (Goodness of Fit Index) value and AGFI (Adjusted Goodness of Fit Index) value is greater than 0.90 which represent it is a good fit. The calculated CFI (Comparative Fit Index) value and NFI (Normed Fit Index) values are greater than 0.90 which means that it is a perfectly fit. It is found that RMSEA (Root Mean Square Error of Approximation) value is 0.000 and RMS (Root Mean Square) value is 0.059, which is less than 0.08, which indicates it is perfectly fit.

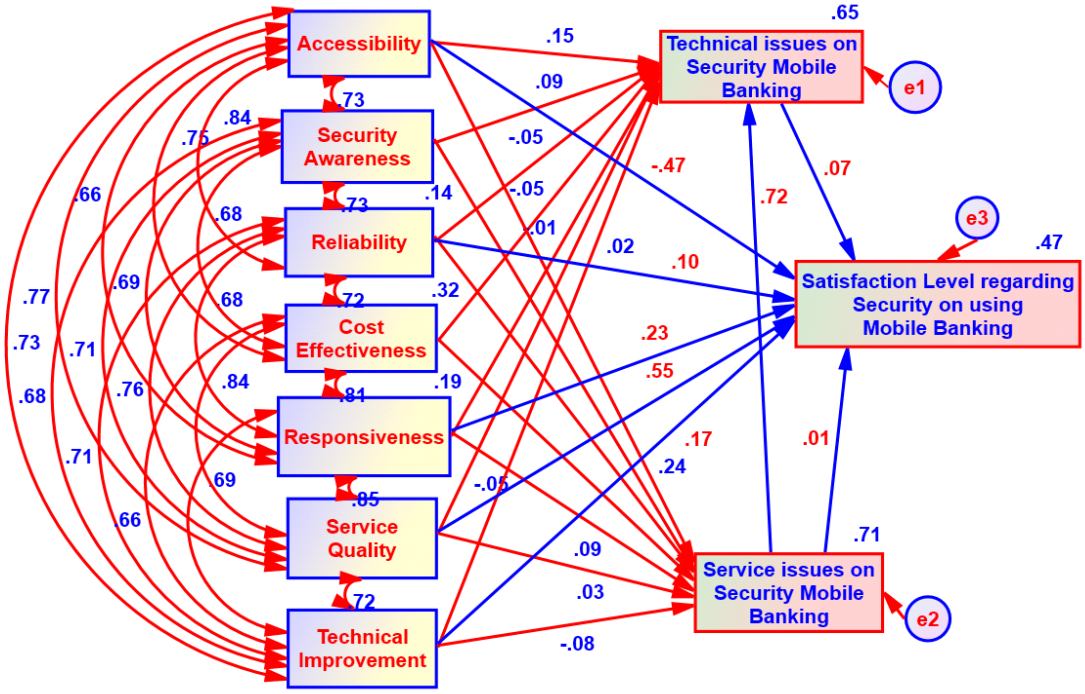

Fig. I. Model Fit.

Table II. Regression Weights

DV	Path	IV	Estimate	S.E.	C.R.	B	p
Service factors on security mobile banking	<---	Accessibility	.194	.044	4.387	.243	0.000
Service factors on security mobile banking	<---	Security Awareness	.110	.033	3.322	.145	0.000
Service factors on security mobile banking	<---	Reliability	.285	.048	5.963	.317	0.000
Service factors on security mobile banking	<---	Cost Effectiveness	.157	.045	3.447	.185	0.000
Service factors on security mobile banking	<---	Responsiveness	.069	.041	1.681	.092	.093
Service factors on security mobile banking	<---	Service quality	.017	.038	.447	.028	.655
Service factors on security mobile banking	<---	Technical Improvement	-.043	.023	-1.843	-.079	.065
Technical factors on security mobile banking	<---	Accessibility	.147	.059	2.470	.155	.013
Technical factors on security mobile banking	<---	Security Awareness	.084	.044	1.909	.093	.056
Technical factors on security mobile banking	<---	Reliability	-.049	.065	-.745	-.046	.456
Technical factors on security mobile banking	<---	Cost Effectiveness	-.055	.061	-.911	-.055	.362
Technical factors on security mobile banking	<---	Responsiveness	-.007	.054	-.126	-.008	.900
Technical factors on security mobile banking	<---	Service quality	-.036	.050	-.708	-.048	.479
Technical factors on security mobile banking	<---	Technical Improvement	.010	.031	.324	.016	.746
Technical factors on security mobile banking	<---	Service factors on security mobile banking	.852	.064	13.302	.718	0.000
Security satisfaction level regarding use of mobile banking	<---	Technical Improvement	.209	.070	2.965	.172	.003
Security satisfaction level regarding use of mobile banking	<---	Service quality	.761	.111	6.870	.549	0.000
Security satisfaction level regarding use of ATM	<---	Responsiveness	.379	.117	3.230	.225	.001
Security satisfaction level regarding use of mobile banking	<---	Reliability	.203	.149	1.361	.101	.174
Security satisfaction level regarding use of mobile banking	<---	Technical factors on security mobile banking	.124	.112	1.110	.066	.267
Security satisfaction level regarding use of mobile banking	<---	Service factors on security mobile banking	.028	.173	.160	.012	.873
Security satisfaction level regarding use of mobile banking	<---	Accessibility	-.844	.135	-6.240	-.472	0.000

Considering the significant individual path coefficients, it is seen that the influence of independent variables on service factors on security mobile banking, accessibility shows

(C.R. – 4.387, beta – 0.243, p – 0.000), security awareness shows (C.R. – 3.322, beta – 0.145, p – 0.000), reliability shows (C.R. – 5.963, beta – 0.317, p – 0.000) and cost effectiveness shows (C.R. – 3.447, beta – 0.185, p – 0.000). Hence the p values are less than 0.05 and the hypotheses are rejected and significant influence over service factors on security mobile banking at 1% level. Other remaining independent variables are responsiveness, service quality and technical improvement not influence over dependent variable of service factors on security mobile banking.

Considering the significant individual path coefficients, it is seen that the influence of independent variables on technical factors on security mobile banking, accessibility shows (C.R. – 2.470, beta – 0.155, p – 0.013) and service factors on security mobile banking shows (C.R. – 13.302, beta – 0.718, p – 0.000). Hence the p values are less than 0.05 and the hypotheses are rejected and significant influence over technical factors on security mobile banking at 1% level. Other remaining independent variables are security awareness, reliability, cost effectiveness, responsiveness, service quality and technical improvement not influence over dependent variable of technical factors on security mobile banking.

Considering the significant individual path coefficients, it is seen that the influence of independent variables on satisfaction level regarding security on using mobile banking, technical improvement shows (C.R. – 2.965, beta – 0.172, p – 0.003), service quality shows (C.R. – 6.870, beta – 0.549, p – 0.000), responsiveness shows (C.R. – 3.230, beta – 0.225, p – 0.001) and accessibility shows (C.R. – -6.240, beta – -0.472, p – 0.000). Hence the p values are less than 0.05 and the hypotheses are rejected and significant influence over on satisfaction level regarding security on using mobile banking at 1% level. Other remaining independent variables are reliability, technical factors on security mobile banking and service factors on security mobile banking not influence over dependent variable of satisfaction level regarding security on using mobile banking.

Relationship between Service quality and Technical Improvement (C.R. = 11.991, r = 0.720 and p = 0.000), relationship between Service quality and Responsiveness (C.R. = 13.260, r = 0.847 and p = 0.000), relationship between Responsiveness and Cost Effectiveness (C.R. = 12.915, r = 0.810 and p = 0.000), relationship between Cost Effectiveness and Reliability (C.R. = 12.011, r = 0.722 and p = 0.000), relationship between Reliability and Security Awareness (C.R. = 12.142, r = 0.734 and p = 0.000), relationship between Security Awareness and Accessibility (C.R. = 12.065, r = 0.727 and p = 0.000), relationship between Technical Improvement and Accessibility (C.R. = 12.064, r = 0.727 and p = 0.000), relationship between Technical Improvement and Security Awareness (C.R. = 11.581, r = 0.684 and p = 0.000), relationship between Technical Improvement and Reliability (C.R. = 11.919, r = 0.714 and p = 0.000), relationship between Technical Improvement and Cost Effectiveness (C.R. = 11.360, r = 0.665 and p = 0.000), relationship between Technical Improvement and Responsiveness (C.R. = 11.656, r = 0.690 and p = 0.000 relationship between Service quality and Accessibility (C.R. = 12.492, r = 0.767 and p = 0.000), relationship between Service quality and Security awareness (C.R. = 11.918, r = 0.714 and p = 0.000), relationship between Service quality and Reliability (C.R. = 12.416, r = 0.760 and p = 0.000), relationship between Service quality and Cost Effectiveness (C.R. = 13.180, r = 0.838 and p= 0.000), relationship between Responsiveness and Accessibility (C.R. = 11.339, r = 0.663 and p = 0.000), relationship between Responsiveness and Security Awareness (C.R. = 11.656, r = 0.690 and p = 0.000), relationship between Responsiveness and Reliability (C.R. = 11.569, r = 0.683 and p = 0.000), relationship between Cost Effectiveness and Accessibility (C.R. = 12.283, r = 0.747 and p = 0.000), relationship between Cost Effectiveness and Security Awareness (C.R. = 11.488, r = 0.676 and p = 0.000), relationship between Reliability and Accessibility (C.R. = 13.188, r = 0.839 and p = 0.000). Hence the p values are less than 0.05 and the hypotheses are rejected. It is concluded that positive relationship among the variables.

1.4 Findings

Service factors that influencing on security of e-banking is significant with reliability and cost effectiveness of e-banking service. Technical factors of e-banking security services are significant with easy accessibility of security systems provided by the bankers, cost

effectiveness of the services and system server responsiveness. Service quality of the e-banking security system is highly significant with technical factors and technical improvement activities done by the service provider banks.

Satisfaction of customers towards e-banking security system is significant with service quality, technical improvement activities and responsiveness of system server and easy accessibility of system.

IV. Suggestions

- E-banking security system should be reliable with customers' standards and their profile. It should alter based on their individual needs and expertise.
- E-banking security system should be easy accessible by ordinary person who have the customers of their bank, highly complicated system administration may lose their customers.
- E-banking security system should be affordable cost with respect to their security system. High cost may charge by the service provider bank, customers may shift their banking activities to other low cost providers.
- E-banking security system should be high speed responses, due to security issues, it may take more time to response, and customer may get irritation.

Further Recommended solution for secured Electronic banking transaction via Mobile, SMS and Phone Banking:

- Banks to develop and install anti-virus software which is embedded in the banking app itself so that in case if the mobile is affected with virus at least the banking app doesn't get hacked / hampered. Also banks giving recommendation of anti-virus software and if possible to send app/link to customers for installing in mobile phones which will be security for customers and for mobile/SMS banking from mobile cyber crime activities.
- Banks to have security pass code and biometric recognition for securing the mobile app program at each level to make it more secured. Also to create a unique identification on mobile banking app and informed the same to customers that if present it is the original banking app.
- Also to use encryption format wherein if the bank credentials or auth code is given it is encrypted in a code format and sent to the bank servers so that it is difficult to be tracked/traced when the credentials are entered.
- To develop biometric app which can be installed in all the mobile phone wherein it can detect fingerprint recognition, face recognition, voice recognition and it can be used for security purpose like unlocking mobile phone, for logging into mobile app, emails and if required even accessing messages/SMS, downloads, e-payments etc. Since by using multiple and different security passwords and biometric at each level will reduce hacking of mobile phones
- The banks to send precautionary steps/measures to the customers every quarter via SMS, mail or else pop up window on click of mobile app etc and display in TV of every bank branch on the various cyber threats and the measures to be taken like
- Just for the sake of convenience not to keep emails and other apps constantly open but to sign in when required and to sign out immediately when completed.
- Ensure that mobile data backup is taken regularly and formatted/scanned for anti-virus scan and ensure the mobile is kept with you and don't leave it unattended even for 5mins.
- In case if the mobile is lost and found then immediately do the anti-virus scan and re-format the mobile etc.
- Banks, RBI and government to keep a separate cyber team customer support apart from Cyber Police for the reach of the public with an emergency no. like 1001 or 500 etc, so that in case of any cyber threats or issues the customers can immediately call to that no. without any hesitation and for tracking the missing phone whereabouts and in case if it is a major threat then the cyber team transfer the case to cyber police. Also checking the security perspective of the mobile banking app if it is secured from modern cyber-attacks etc. Also to create a website wherein the customers can register their mobile no. so that in case of loss of mobile it be traced with the help of mobile network or GPS

V. Conclusion

Mobile, SMS and Phone banking is one of the user friendly banking technologies for bank and customers. Many innovative Banking features and banking services are being added and incorporated in the mobile banking. But on the contrary there is a rise of cyber-crimes/frauds/threats and if banks and customer adhere strictly the precautionary steps and security measures then surely even more major development/innovation will be taking place for advanced user friendly digitized electronic payment transactions at merchant/vendor outlet.

VI. References

[1]. Harshad Patel and Vijay Pithadia, "Emerging Trends in Customer Satisfaction of Value Added Services in Selected Banks at Mehsana District of Gujarat", International Monthly Refereed Journal of Research in Management & Technology, Volume - 2, June - 2013, pp 9-16., 2013

[2]. Shumaila Y. Yousafzai, John G. Pallister, Gordon R. Foxall,"A proposed model of e-trust for electronic banking" Technovation, 23, Pg. 847-860, 2003

http://business.cf.ac.uk/sites/default/files/A_proposed_model_of_etrust_for_electronic_banking.pdf

[3]. Tommi, L. (2007), *"Internet Vs Mobile banking: Comparing customer value perceptions*", Business Process Management Journal, 13(6), 788-796.

[4]. Ravi V, Mahilcarr and Sagar N.V (2008), *"Profiling of Internet Banking Users in India using Intelligent Techniques"*, Journal of Services Research, Volume – 6, Issue - 2, pp 61-72

[5]. Vanessa Pegueros (2012), "Security of Mobile Banking and Payments", Sans Institute infoSec Reading room

https://www.sans.org/reading-room/whitepapers/ecommerce/security-mobile-banking-payments-34062

[6]. Thakur, Rakhi and Srivastava, Mala (2013), *"Customer usage intention of mobile commerce in India: an empirical study"*, Journal of Indian Business Research Vol. 5 No. 1, pp. 52-72.