Customer Perception on Security Systems in E-Banking Services with special references to ATM

P. Sailaja and Dr. V. Thamodaran
1PhD Research Scholar, Dept. of Business Administration, Annamalai University, Annamalainagar
2Assistant Professor, Dept. of Business Administration, Annamalai University, Annamalainagar

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 and vastly used in E-banking technology is ATM (Automated Teller Machine). The other major E-Banking services are internet/online banking, Net banking, Mobile banking, SMS banking, Phone banking, swiping card via EDC machine at vendor outlet etc. This paper has dealt with customers' satisfaction towards security system in ATM as part of e-banking and its preventive measures.

Introduction

1.1 Concept of E-Banking

E-Banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. Customers access E-Banking services through various technology and devices like ATM, Internet/Online banking, Net banking, Kiosk, Mobile and Phone banking. 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 maintaining 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) (1965-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.

Initially Japan, Sweden, UK and US developed envelope deposit machine in 1960 under Luther George Simjian part of Simjian Reflectone Electronics Inc. and installed in City bank of New York, but it is not much successful. In the same year i.e. 1960 Japan, Sweden and Britain developed under the invention of John Shepherd-Barron, a cash dispensing machine and installed in Barclays Banks. This cash dispensing machine is developed after development of electronic fund transfer; but there is a slowdown for acceptance and enhancement of using Cash dispensing machine. Later on it is converted into ATM and used by the Banks wherein it started developing rapidly with new features and widely spread in the banking sector worldwide wherein currently almost every bank have an ATM center.

On the contrary there is a development of Biometric technology in mid 1980s/20th Century.
Based on this Bio-Metric ATM is developed and introduced in Poland by ITCARD, Bangladesh, and Cambodia by ITC and also introduced in Pune, India by Axis software and installed in Punjab National Bank. This Bio-metric ATM is currently spreading and many banks are in a verge of introducing this Bio-Metric ATM even though it is costly than the current ATM.

1.3. Automated Teller Machine (ATM)

Automated Teller Machine is a computerized machine which is installed by Banks at various locations wherein the customers with the help of ATM Debit / credit card or account no. can facility ATM for accessing their account, dispensing cash, transfer funds, to carry out other financial & non-financial transactions and even apply for new financial product or services etc. without the need to actually visit their bank branch. Since the ATM is present 24/7*365 days round the clock and can do banking activities at any ATM centre irrespective of the bank as long as debit/credit card are tied up with Visa/Maestro etc., it has become user friendly to the customers and hassle free. For transacting at an ATM, the customer inserts /swipes his card in the ATM and enters his Personal Identification Number (PIN) issued by his bank. Once PIN is accepted by ATM a customer can perform the transaction selected by him. This has reduced manpower i.e. teller, clerk, withdrawal of cash, long queue, and other miscellaneous banking services or transactions without visiting the bank. Currently Bio metric ATM is used for secured ATM with a motto to reduce cyber-crime/frauds. Bio metric is usage of identification system for our unique selves like using scanning/recognizing of body parts like retina, iris, voice, fingerprint, face, skin, hair etc. Currently even bank employees are using bio-metric finger print device for operating or while handling/depositing cash in ATM centres.

Common cyber-attack/threats/frauds in e-banking causing a security breach in ATM:

Even though there is a rise in technology for providing convenience to the customer for user-friendly banking on the contrary there is a rise in cyber-crime/threats/frauds. E-Banking is one of the targeted cyber-crime in order to steal customer account details, money etc. List of Cyber-crimes/threats/frauds in ATM are:

- Robbery of cash in ATM by stealing Cash from ATM machine either in prime or mainly in remote locations.
- Withdrawal of cash from ATM by attacking the customers at gunpoint
- Criminals attacking the ATM centers at the time of cash transit or during the time of cash deposit into the ATM machine by the bank officials causing a huge loss of money
- Using Skimming device attached to the slot machine to read the debit/credit card details.
- Camera and tracer / fingerprint masking / key pad electronic device/ spy cameras to view and track the ATM PIN no./ device to track chip and magnetic strip debit/credit card details
- Hackers Creating a duplicate debit / credit card based on the details from the skimming device and the ATM PIN no. tracked via spy camera/device and withdrawal of cash from ATM and shopping at vendor outlet by swiping.
- Security guard are not present / sleeping / away etc. at ATM center by which gives more access for criminals to commit crime at ATM center.
- The surveillance cameras are not periodically checked and not functioning properly creates more criminal crimes wherein advantage for the criminals but huge loss for the banks
- Emergency Alarm systems are not present in most of the ATM centers or not working properly.
- The anti-virus software in the ATM is not up to date from protecting against malware and other virus cyber threats
- Duplicate/dummy ATM centers wherein it looks like original one and wherein it records card details and pin no.

Some of the Precautionary security steps and measures by RBI and Banks for ATM:

- With spread of ATM network instances of frauds are also on the rise. Ensuring secure environment is a must for building customer confidence in electronic banking. The measures initiated to strengthen the security in ATM transactions some of them are enumerated below:
- Caretakers at offsite ATMs and sensitive locations to discourage attempts to tamper with the ATM.
- Arrangements with local police authorities for regular beats in case of ATMs located in sensitive areas.
- Disabling cash retraction facility at ATMs as per RBI guidelines in view of large number of frauds committed by fraudsters taking advantage of this facility
- Security Screen on the Machine requiring the customer to confirm the digits entered
- reduction of per screen transaction time,
Precautionary steps to be taken while using ATM’s

- While performing your transactions at the ATM, do not allow people to look over your shoulder as you enter your PIN. Use your body to block the view others may have as you perform your transaction.
- Memorize your ATM pin and do not write it on your ATM card.
- Change your PIN immediately if you suspect it has been exposed to others or the moment you suspect any unauthorized access. Change your PIN regularly. Never lend your card or disclose your PIN to anyone, including family, friends and people claiming to be bank employees.
- Always take the transaction receipt with you. Do not leave your transaction record at the ATM. Shred it before discarding it.
- If you see anything suspicious while conducting a transaction, cancel your transaction and leave immediately.
- Be aware of your surroundings, particularly at night. If you observe or sense suspicious persons or circumstances, do not use the machine at that time.
- Pay attention to the front of the ATM machine you are using. Does it look different from other ATM’s i.e. does it have a sticky residue on it or extra signage. Familiarize yourself with the look and feel of the ATM machine.
- Never allow a stranger to assist you while using an ATM.
- Do not count or visually display any money you received from the ATM. Immediately put your money into your pocket or purse and count it later.
- Verify the SMS alerts on transactions made on the account and if there any suspicious one, then change the ATM pin and inform the Bank immediately.
- If credit card gets stolen / lost or doesn't function then need a replacement card.

2. Review of Literature

Marshall and Heslop (1988) in their study attempted to investigate the impact of demographic variable on the adoption of ATM services. The study found that consumers’ motives for use of technology were useful for predicting subsequent usage. Demographic factors such as higher education levels and employment status were positively related to usage of ATMs. Age was negatively related to adoption of ATMs.

Leblanc (1990) tried to identify the main consumer motivations for adoption of ATM. Study found out that main consumer motivation for using ATMs was its accessibility benefits. Study also found that used of technology in banking sector improved service quality, presented little security risk and fulfilled their need for simple and fast transactions. Furthermore, non-users preferred interacting with human tellers and perceived ATM usage to be complex and risky.

Lewis (1991) found that users mainly used ATMs for withdrawal of cash and obtaining account balances. Study also found that negative factors regarding ATM usage were concern over personal safety, lack of privacy and operational problems such as machine being regularly out of cash or out of order and cards getting stuck in it.

Rugimbana and Iversen (1994) found that ATM customers mostly used ATMs for cash withdrawal and conducted less than 50% of their transactions through it. The study concluded that most users perceived ATMs to be just convenient cash dispensers, while the non-users preferred contact with human tellers and had a need for personal service. Also the study explored ATM usage entirely from the viewpoint of consumers’ demographics. They examined ATM usage patterns on the basis of consumers’ perceptions. The results based on a survey of 630 retail banking consumers from two separate Australian banking institutions - a bank and a credit union - suggest that ATM users from both institutions differed quite significantly from non-users in their perceptions of at least three ATM attributes; convenience, reliability, and suitability. Furthermore, the results indicate that most users perceive ATMs as mere cash dispensers.

Titrade Cristina (2008) mentioned e-banking advances, focusing general attention on security risks, there could be large security gains. Banks are more benefitted when e-banking increases customer satisfaction. Due to that customers can access their accounts whenever and anywhere thereby creating relationship with banks.
Sunita Bishnoi (2013) elucidated that E-Banking provides various e-channels for using banking services like ATM, credit cards, debit cards, internet banking, mobile banking, electronic fund transfer, electronic clearing system etc. wherein the author mainly focused on ATM/Debit card and the customer perception and the various issues of using ATM services. The author collected data and analyzed with the help of SPSS and statistical techniques and based on findings the customers feel the ATM useful and is helpful in performing the various transactions like friendly ATM, withdrawal at any bank ATM, reduces cash requirement, no extra cost from bank side, convenient while traveling, bill payment via ATM and using debit card at vendor outlet for purchases, transfer of funds and other specialized services of ATM to customers. But on the contrary the problem faced by customers while using ATM services are like machine out of cash, out of order, poor visibility of statement slip, no printing of statement, cards get blocked, difficulty in swiping or retrieving the cards etc. and thus the banks should work towards resolving the problem areas and to provide better ATM services to customers.

3. Research Methodology and Analysis

3.1. Objective:
To analyze the factors that influences the security system of ATM a part of e-banking services and also to evaluate customers’ satisfaction towards various factors of security system in e-banking services

3.2. 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 Security satisfaction level regarding use of ATM. 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 ATM and Technical factors on security ATM.

3.3. Model Fit

From the above table it is found that the calculated chi-square value is 0.744, p value is 0.295 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, which is less than 0.08, which indicates it is perfectly fit.

Figure 1. Model Fit.

Regression Weights

Table 2. Regression Weights
Considering the significant individual path coefficients, it is seen that the influence of independent variables on service factors on security ATM, service security awareness shows (C.R. = 2.178, beta = 0.102, p = 0.029), reliability shows (C.R. = 4.333, beta = 0.425, p = 0.000), cost effectiveness shows (C.R. = 5.867, beta = 0.392, 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 ATM at 1% level. Other remaining independent variables are accessibility, responsiveness, service quality and technical improvement not influence over dependent variable of service factors on security ATM.

Considering the significant individual path coefficients, it is seen that the influence of independent variables on technical factors on security ATM, accessibility shows (C.R. = 5.419, beta = 0.212, p = 0.000), cost effectiveness shows (C.R. = 2.183, beta = 0.086, p = 0.029), responsiveness shows (C.R. = 2.454, beta = 0.095, p = 0.014), service quality shows (C.R. = 3.530, beta = 0.154, p = 0.000), technical improvement shows (C.R. = 2.762, beta = 0.084, 54 = 0.006) and service factors on security ATM shows (C.R. = 22.627, beta = 0.724, 54 = 0.000). Hence the p values are less than 0.05 and the hypotheses are rejected and significant influence over on technical factors on security ATM at 1% level. Other remaining independent variables are security awareness and reliability not influence over dependent variable of technical factors on security ATM.

Considering the significant individual path coefficients, it is seen that the influence of independent variables on Security satisfaction level regarding use of ATM, technical improvement shows (C.R. = 3.790, beta = 0.197, p = 0.000), service quality shows (C.R. = 7.119, beta = 0.510, p = 0.000), responsiveness shows (C.R. = 4.623, beta = 0.292, p = 0.000), accessibility shows (C.R. = 8.177, beta = 0.547, p = 0.000) and Technical factors on security ATM shows (C.R. = 4.003, beta = 0.342, p = 0.000). Hence the p values are less than 0.05 and the hypotheses are rejected and significant influence over on security satisfaction level regarding use of ATM at 1% level. Other remaining independent variables are reliability and service factors on security ATM not influence over dependent variable of Security satisfaction level regarding use of ATM.

Relationship between Service quality and Technical Improvement shows (C.R. = 11.991, R = .720 and p = 0.000), relationship between Service quality and Responsiveness shows (C.R. = 13.260, R = .847 and p = 0.000), relationship between Responsiveness and Cost Effectiveness shows (C.R. = 12.915, R = .810 and p = 0.000), relationship between Cost Effectiveness and Reliability shows (C.R. = 12.011, R = .722 and p = 0.000), relationship between Reliability and Security Awareness shows (C.R. = 12.142, R = .734 and p = 0.000), relationship between Security Awareness and Accessibility shows (C.R. = 12.065, R = .727 and p = 0.000), relationship between Technical Improvement and Accessibility shows (C.R. = 12.064, R = .727 and p = 0.000), relationship between Technical Improvement and Security Awareness shows (C.R. = 11.581, R = .684 and p = 0.000), relationship between Technical Improvement and Reliability shows (C.R. = 11.919, R = .714 and p = 0.000), relationship between Technical Improvement and Cost Effectiveness shows (C.R. =11.360, R = .665 and p = 0.000), relationship between Technical Improvement and Responsiveness shows (C.R. = 11.656, R = .690 and p = 0.000), relationship between Service and Accessibility shows (C.R. = 12.492, R = .767 and p = 0.000), relationship between Service quality and Security Awareness shows (C.R. = 11.918, R = .714 and p = 0.000), relationship between Service quality and Reliability shows (C.R. = 12.416, R = .760 and p = 0.000), relationship between Service quality and Cost Effectiveness shows (C.R. = 13.180, R = .838 and p = 0.000), relationship between Responsiveness and Accessibility shows (C.R. = 11.339, R = .663 and p = 0.000), relationship between Responsiveness and Security Awareness shows (C.R. = 1.656, R = 0.690 and p = 0.000), relationship between Responsiveness and Reliability shows (C.R. = 11.569, R = .683 and p = 0.000), relationship between Cost Effectiveness and Accessibility shows (C.R. = 12.283, R = 0.747 and p = 0.000), relationship between Cost Effectiveness and Security Awareness shows (C.R. = 11.488, R = .676 and p = 0.000) and relationship between Reliability and Accessibility shows (C.R. = 13.188, R = .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.

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.
5. 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.

Recommended Solution for secured ATM Transactions:

- Bio Metric to be incorporated in all ATM centre like Voice/retina/ Iris /face/Palm/finger/skin which is reads via laser sensors at entry/exit door, ATM cash deposit slot(by banks), ATM transactions by customers i.e. Bio-metric ATM machine compulsorily

- Instead/apart from ATM Pin No. to use OTP PIN or Answer 4 secret questions which is single digit number or Biometric recognition or a combination of all the 3.

- To use sensors for reading card instead of swiping like waving of card or display like access card to be incorporated compulsorily

- Laser beam sensors at entry door of ATM Centre and at ATM machines which allows only 1 person or based on no. of ATMs machines and if exceeds beep sound is generated. If persist more than 2-5 mins automatically door closes and can be opened only by bank officials. Also to incorporate automatic laser sensor doors for detecting no. of person entry into ATM centre.

- To install spy camera both inside and outside ATM centre apart from CCTV camera by bank officials

- To install Alarm system/alarm button/alarm 4 digit no. at entrance and ATM machine wherein if triggered it sends buzzer/SMS/call to bank official and authorized private security and if required police

- In case of emergency/alarm buzzer then automatically ATM door is closed, ATM machine gets shutdown/hibernate and the bank officials, Authorized private security & if required police to be present immediately within 2-5mins by following the escalation matrix

- To install skimming prevention software, anti-virus software and touch pad prevention software to protect from malware attack and also it gets shaken and interrupts the scanning process while insert/exist of the card and punching the PIN no. making the cyber-crime ineffective.

- To have unique hologram stickers or identification on Debit/credit card and ATM Machines. Also a sensor placed in ATM machine card slot which recognizes the unique identification on the card, also helps vendor in identification

- To have quality audit check and mock drill periodically on the security systems in the ATM centres by not only bank officials but also by police/Private security agency with special privileges.

- A phone to be installed in all ATM and an emergency contact no. similar to 100 e.g. 500, 1000 etc. to be provided by the banks/RBI, this needs to be notified to customers and displayed in ATM centres.

- To stick precautionary steps to be taken by customers along with emergency contact no. especially on the ATM Machine apart from notice board in ATM centres.

- Copy of Back ground check report of bank officials, security guard and technicians etc. to be sent periodically to police department for verification.

- Bank officials to use Bio-metric devices for the cash chest during money transfer/deposit and to change Security guard/bank officials monthly and cash deposit timings by bank officials in ATM centres.

6. Conclusion

ATM is one of the user friendly banking technologies for both bank and customers. Many innovative features and banking services are being added and incorporated in the ATM thereby moving towards digitized ATM center. But on the contrary there is a rise of ATM 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 ATM center.

7. REFERENCES


