CUSTOMER PERCEPTION ON SECURITY SYSTEM IN E-BANKING SERVICES WITH SPECIAL REFERENCES TO EDC

P. Sailaja,

PhD Research Scholar
Dept. of Business Administration,
Annamalai University, Chidambaram, India

Dr. V. Thamodaran,

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 and vastly used in combination of E-commerce and E-banking technology is EDC (Electronic Data Capture) i.e. Card Swiping Machine in Vendor Outlet. For payment transactions at vendor outlet i.e. shopping etc. the debit/credit card is swiped via EDC machine and after few authentication code given by customer and vendor the amount is directly debited from customer account and credited to vendor account as per the banking regulations timeframe. This helps in reducing the handling or carrying cash and transparency of cash transactions for both to the vendor and the customers. 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.

Keywords: Security system in EDC or Card swiping Machine or POS.

Introduction:
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 evironment 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.

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) (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.

The EDC machine is evolved based on RDE (Remote Data Entry) machine used for clinical research data in 1970's by Institute of Biological research and Development (IBRD). After the evolution of internet in mid 1990 it is been converted into EDC which is been used with the help of electronic web based software. Based on this EDC machine some of the software companies, pharmaceuticals, biotech, contact research organization and banks have developed their own EDC machine in respective sectors.

The credit card originated in 1920 by individual firms and the bank credit card in 1946 by John C. Biggins at Flatbush National Bank of Brooklyn, New York which then introduced the first ever general purpose credit card in year 1952, based on this Bank of America and other banks collaborated formed 2 groups and issued international credit/debit card called Visa and Master card which now currently used worldwide. Currently smart card which uses computer chips and biometrics etc is introduced in 2013-2014 in UK and now being used worldwide.

The EDC machine which is also called as Card swiping machine and PDQ (Process data quickly) was developed by IBM for catering the banking industry and was first introduced in USA merchant/retail outlets. The EDC machine is a portable machine connected via EDC software wireless internet connection and used in all merchant/vendor outlets. This helps in cashless transaction/cash handling by just swiping credit/debit/smart cards and making purchases etc at merchant/vendor outlet making it more convenient for the customers and the merchant/vendor.

In recent development card swiping is done by swiping slot attached to iphone/smart phones and attached to laptop/computer monitor.

Electronic Data Capture (EDC):

An EDC i.e. Electronic Data Capture is a machine used to facilitate debit or credit card payments either via swiping or dipping or inserting. It is also called as Credit card swipe machine or Debit card Swipe machine. In Case if the EMV chip is present on the card it is inserted/dipped, if not then it is swiped where the magnetic strip is present back side of the card. This swiping machine is mostly used at vendor outlets i.e. hotels, grocery shops, petrol bunks and other retail shops etc. This helps customers in reducing fear, theft etc. for carrying huge amount of cash and making it convenient for purchasing goods or services. It also helps the vendor from misuse of cash by cashier, less handling of cash and direct credit to the merchant bank account with transparency of cash tracking transaction.

The other terminologies used are Magnetic stripe card reader - magnetic stripe on the back side of the debit/credit card is used. EFTPOS – Electronic fund transfer at point of sale or POS – Point of Sale – wherein the EMV chip is embedded on the debit/credit card is used.

The customer swipes or dip the debit/credit/smart card via EDC machine, the vendor then enters his merchant code, pin no., CVV no. on back side of the card and then the customer punch in the ATM PIN Number. The EDC machine reads the credit/debit card no., the 3 digit CVV no. punched by the merchant/vendor, the magnetic strip code or code from EMV chip, issue/expiry date, customer name etc. and then this is being transmitted to the merchant service provider which then checks the details and transmit the amount to the merchant account sometimes immediately or after 24/48 hours and 2 slips are generated as a confirmation i.e. customer copy and a merchant copy and even an SMS is sent to the customer registered mobile no. The merchant verifies if the signature of the customer signature signed on the merchant copy matches with the signature on the back side of the card. And all of these are processed and checked under a minute/within seconds.

UK is the first country introducing the EMV chip in debit/credit card wherein the no. /details changes for every transactions and PIN no. is punched. There is EMV Chip and Pin and Chip and signature. Many countries have started using / introducing including India on EMV chip debit/credit card apart from Magnetic strip card. US are planning to make EMV chip and Pin mandatory from 2015-2016 and stop Magnetic strip card.

As per India RBI regulations implemented stating after swiping the card to enter the ATM PIN no. to make it secured. But this became an advantage for the criminals and hackers thereby increasing the rise in cyber-crime frauds.

Many Cyber frauds/attacks are taking place during the time of swiping debit/credit card while using swiping

machine by using skimming device and tracking the ATM PIN Number via CCTV or noting down while customer is entering the details thereby increasing a rise in the crime by creating duplicate card and withdrawing huge amount of cash via ATM or online/offline shopping. Even the EMV chip and PIN are prone to future attacks like cloning the EMV Chip, Malware attack chips, cryptogram is not checked properly by banks and devices for hacking the EMV chip since based on research it seems there are flaws in POS system.

Some of the precautionary security steps and measures by RBI and Banks for EDC:

With spread of EDC/Card swiping machine/electronic payment transaction terminals the 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 EDC/Electronic payment transactions are enumerated below:

- Issued orders to Banks to issue and replace magnetic strip debit/credit card with EMV chip debit/credit card especially for the cards used internationally. Since this reduces the cyber fraud to some extent.
- To use ATM PIN no. as an authentication for while making electronic payment transaction via EDC machine at vendor/merchant outlet
- Banks to ensure that the EDC machine/terminals and the IP address are certified by PCI-DSS (Payment card Industry-Data Security Standards) and PA-DSS (Payment Applications-Data Security Standards)
- Instant SMS facility for payment transactions and for blocking the cards instantly in case of loss of card by customers
- To provide option to customer to have upper limit cap on the payment transaction/mode of transaction/beneficiary while using EDC or other Ebanking transactions.
- Banks to incorporate and move towards the fraud monitoring system and to take measures and rules on curbing the cyber-crime bank frauds.

Customer and Vendor Awareness and Education Measures:

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:

- Customers to check if the Visa or Master card or Maestro sticker is present on the EDC machine
- The customers always ensure that while making payment at EDC/POS the card is swiped in their presence only.

- Do not share PIN, CVV or any security information related details with anyone.
- To cover with hand etc while punching ATM pin no. on the EDC machine during payment transactions.
- Always check Debit card when returned after purchase.
- Insist for a copy of the receipt and retain it till the account statement is checked.
- Please assure yourself about the genuineness of the merchant beforehand.
- Vendors to submit MIS and backup data files accordingly to bank either daily/weekly/month etc.
- Vendor to ensure strict confidentially of information or data provided by the banks even though the contract is expired or present and also allow for audit checks by banks, RBI and other quality audit officials etc.
- Banks to inspect on time to time basis on the EDC machine, security of data, storage of information, handling of data etc as per the banks and statutory legal requirements.

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[2] and N.B.Jadhav et. al, 2011)[3] 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.

(Titrade Cristina et.al, 2008)[3] mentioned e-banking advances, focusing general attention on security risks, there could be large security gains. Banks are more benefitted when e-banking is increases customer satisfaction. Since due to that customers can access their accounts whenever and anywhere thereby creating relationship with banks.

(Dr.S.Gurusamy, 2009)[4] Mentioned that in seventies the evolution of electronic card authorization systems, electronic clearing and settlement systems and electronic data capture (EDC) at the point of sale system (POS) terminals. This lead to less paper work and significantly speeded the process.

(Swara, 2012)[5] explained about the credit card swiping machine/EDC and its functionality, and the eligibility requirement and application procedure for procuring credit card swiping machine/EDC/PDQ by the vendor/merchant/business. The Credit card and EDC machine made convenient to customers for less cash handling facility and purchasing goods and services at various retail store, dining establishments, car showroom etc. but on the contrary there is a fear of credit card being misused / stolen. Explained about how the EDC machine reads the card details like name, expiry date and card no. and for verification PIN no. is punched it which then sends these details to merchant service provided and is being processed within seconds for transaction getting completed.

(Preeti Kulkarni, 2013)[6] explained the difference and security measures of EMV chip against the magnetic stripe debit/credit card wherein it is difficult to track the card details which has EMV chip via skimming machine or read card details thereby reducing the cyber-crime frauds. The reason behind is that EMV chips have embedded micro-processors and is capable of storing and transaction data in an encrypted, tamper-proof format protecting card holders from sundry security threats. However chip-based card is no

guarantee against fraud and hence precautions needs to be taken of not disclosing CVV no., PIN no. or other confidential details to others since technology no matter how robust will not be able to come to rescue.

Research Methodology and Analysis:
Objective:

To analyze the factors that influences the security system of EDC a part of e-banking services and also to evaluate customers' satisfaction towards various factors of security system in e-banking services

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 credit card / EDC. 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 EDC and Technical factors on security EDC.

Model Fit:

Table 1: Model Fit

Chi-Square	p	DF	RMSEA	GFI	AGFI	CFI	NFI
3.782	0.151	1.891	0.046	0.998	0.951	1.000	0.999

From the above table it is found that the calculated chi-square value is 3.782, p value is 0.151 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 0.046, which is less than 0.08, which indicates it is perfectly fit.
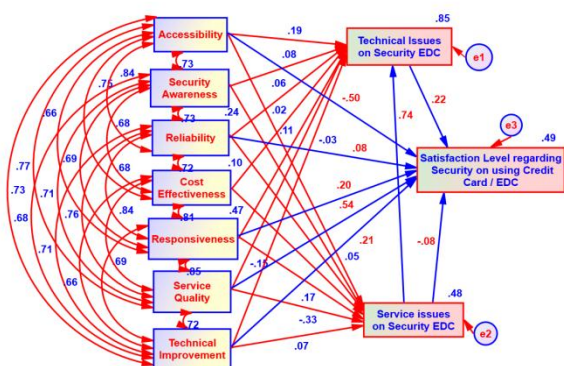
Fig. I: Model Fit.

Table 2: Regression Weights

DV		IV	Estimate	S.E.	C.R.	B	p
Service factors on security EDC	←	Accessibility	.038	.056	.671	.050	.502
Service factors on security EDC	←	Security Awareness	.170	.042	4.046	.237	0.000
Service factors on security EDC	←	Reliability	.082	.060	1.362	.097	.173
Service factors on security EDC	←	Cost Effectiveness	.371	.058	6.457	.466	0.000
Service factors on security EDC	←	Responsiveness	.118	.052	2.268	.167	.023
Service factors on security EDC	←	Service quality	-.190	.048	-3.921	-.325	0.000
Service factors on security EDC	←	Technical Improvement	.036	.030	1.205	.070	.228
Technical factors on security EDC	←	Accessibility	.133	.028	4.708	.188	0.000
Technical factors on security EDC	←	Security Awareness	.054	.022	2.501	.080	.012
Technical factors on security EDC	←	Reliability	.044	.030	1.457	.056	.145
Technical factors on security EDC	←	Cost Effectiveness	.014	.030	.463	.019	.643
Technical factors on security EDC	←	Responsiveness	.070	.026	2.667	.106	.008
Technical factors on security EDC	←	Service quality	-.083	.025	-3.336	-.151	0.000
Technical factors on security EDC	←	Technical Improvement	-.014	.015	-.941	-.029	.347
Technical factors on security EDC	←	Service factors on security EDC	.690	.024	28.223	.738	0.000
Security satisfaction level regarding use of EDC	←	Technical Improvement	.261	.069	3.790	.215	0.000
Security satisfaction level regarding use of EDC	←	Service quality	.754	.109	6.896	.545	0.000
Security satisfaction level regarding use of EDC	←	Responsiveness	.340	.118	2.887	.203	.004
Security satisfaction level regarding use of EDC	←	Reliability	.159	.140	1.134	.079	.257
Security satisfaction level regarding use of EDC	←	Technical factors on security EDC	.569	.226	2.523	.224	.012
Security satisfaction level regarding use of EDC	←	Service factors on security EDC	-.200	.192	-1.042	-.084	.297
Security satisfaction level regarding use of EDC	←	Accessibility	-.897	.131	-6.820	-.502	0.000

Considering the significant individual path coefficients, it is seen that the influence of independent variables on service factors on security EDC, security awareness shows (C.R. – 4.046, beta – 0.237, p – 0.000), cost effectiveness shows (C.R. – 6.457, beta – 0.466, p –

0.000), responsiveness shows (C.R. – 2.268, beta – 0.167, p – 0.023) and service quality shows (C.R. – -3.921, beta – -0.325, 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 EDC at 1% level. Other remaining independent variables are accessibility, reliability and technical improvement not influence over dependent variable of service factors on security EDC.

Considering the significant individual path coefficients, it is seen that the influence of independent variables on technical factors on security EDC, accessibility shows (C.R. – 4.708, beta – 0.188, p – 0.000), cost effectiveness shows (C.R. – 2.501, beta – 0.080, p – 0.0120), responsiveness shows (C.R. – 2.667, beta – 0.106, p – 0.008), service quality shows (C.R. – -3.336, beta – -0.151, p – 0.000) and service factors on security ATM shows (C.R. – 28.223, beta – 0.738, 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 EDC at 1% level. Other remaining independent variables are reliability, cost effectiveness and technical improvement not influence over dependent variable of technical factors on security EDC.

Considering the significant individual path coefficients, it is seen that the influence of independent variables on satisfaction level regarding security on using credit card / EDC, technical improvement shows (C.R. – 3.790, beta – 0.215, p – 0.000), service quality shows (C.R. – 6.896, beta – 0.545, p – 0.000), responsiveness shows (C.R. – 2.887, beta – 0.203, p – 0.004), accessibility shows (C.R. – -6.820, beta – -0.502, p – 0.000) and Technical factors on security ATM shows (C.R. – 2.523, beta – 0.224, p – 0.012). 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 credit card / EDC at 1% level. Other remaining independent variables are reliability and service factors on security EDC not influence over dependent variable of satisfaction level regarding security on using credit card / EDC.

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 = .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 = .684 and p = 0.000), relationship between Technical Improvement and Reliability (C.R. =11.919, r = .714 and p = 0.000), relationship between Technical Improvement and Cost Effectiveness (C.R. = 11.360, r = .665 and p = 0.000), relationship between Technical Improvement and Responsiveness (C.R. = 11.656, r = 0.690, 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) and 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.

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.

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 Electronic payment transaction via EDC/POS/Card swiping machine:

- Bio Metric to be incorporated and fixed to EDC/POS/Card Swiping Machine like face/Palm/finger/skin which reads via laser sensors
- Instead of ATM Pin No. to use OTP PIN or alternative PIN no. (Different from ATM Pin No.) or Biometric recognition to be used
- To use sensors for detecting debit/ credit card details by waving of card or card display instead of swiping the card in EDC/Card swipe machine
- Registered mobile to mobile money transfer linked to respective bank account in secure way by entering mobile no., Biometric/pass code, security question and amount details
- Photo mandatory on the Debit/ credit card of the account holder
- Install anti-prevention software in EDC machine to protect from Malware/cyber attacks
- Unique identification on EDC machine and debit/credit card and EDC machine identifying the same
- Quality/surprise audit check at vendor outlet/institutions etc. on no. of EDC machine, and if EDC machine is as per security measure to protect from malpractice etc.
- Precautionary steps display at vendor outlet with emergency contact number and awareness campaign

Conclusion:

EDC/POS/Card swiping machine is one of the user friendly banking technologies for bank, Vendor / Merchant and customers. Many innovative features and banking services are being added and incorporated in the EDC e.g. Payment transaction without debit/credit card, swiping card via card slot attached to smart phones, mobile POS system/MPOS etc. thereby moving towards digitized EDC/POS/Card swiping machine. But on the contrary there is a rise of cyber-crimes/frauds/threats and if banks, Vendor/merchant 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.

References:

[1] Harshad Patel and Vijay Pithadia, (2013). 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.

[2] Shumaila Y. Yousafzai, John G. Pallister, Gordon R. Foxall, (2003). A proposed model of e-trust for electronic banking, Technovation, 23, Pg. 847-860. Available: http://business.cf.ac.uk/sites/default/files/A_proposed_model_of_etrust_for_electronic_banking.pdf

[3] N.B. Jadhav, Mrs. Poonam R. Lohana, Mr. Rupesh Dargad, (2011). "Customer perception and attitude towards e-banking. Published in Management prudence Journal Volume 2 Issue 1002E. Available:http://www.publishingindia.com/mpj/15/customer-perception-and-attitude-towards-e-banking/97/715/

[4] Titrade Cristina, Ciolacu Beatrice, Pavel Florentina, (2008). Ebanking impact, risks, security, Universitatea Romano Americana, volume 4, pg.280. Available: http://steconomice.uoradea.ro/anale/volume/2008/v4-management-marketing/280.pdf

[5] DR. S. Gurusamy, Financial service and systems, [Online], In Tata McGraw-Hill Education Private limited publication, retrieved from https://books.google.co.in/books?id=nPOSoSoRnycC&pg=PA64&dq=electronic+data+capture+machine+evolution&hl=en&sa=X&ei=J8IgVaT4E4qLuASYvICQBQ&ved=0CEcQ6AEwBQ#v=onepage&q=EDC&f=false

[6] Swara, (2012). How A Credit Card Swipe Machine Works [Online] Available:http://www.indiastudychannel.com/resources/151077-How-credit-card-swipe-machine-works.aspx

[7] Preeti Kulkarni, (July 22 2013), Will chip-based cards succeed in reducing credit card fraud? [Online], Published in The Economic times, ET Bureau, 2013, retrieved from http://articles.economictimes.indiatimes.com/2013-07-22/news/40727841_1_sbi-cards-chip-based-cards-emv

*****