FUTURE SCOPE OF E-BANKING IN INDIA

Bhaskar Dutta, Dr. Gajraj Singh Ahirwar, Shyam Sunder Shah
Department of Commerce, UTD, Sri Satya Sai University of Technology and Medical Sciences, Sehore (M.P.), India

ABSTRACT

Today most of the banking happens while you are sipping coffee or taking an important call. ATMs are at your doorstep. Banking services are accessible 24x7. There are more plastic cards in your wallet than currency notes. A huge part of this change is due to advent of IT. Banks today operate in a highly globalized, liberalized, privatized and a competitive environment. In order to survive in this environment banks have to use IT. Indian banking industry has witnessed a tremendous developments due to sweeping changes that are taking place in the information technology.

This work involves descriptive research design as my project is questionnaire based. Descriptive research includes survey and fact- finding enquiries kinds. The major purpose of descriptive research is description of the state of affairs, as it exists at present.

For this study the sample size is 50 people of the area New Delhi, who were using the E-Banking services.

KEYWORDS: *E-banking, bank, technology*

INTRODUCTION

Electronic banking has emerged from such an innovative development. The objective of the present research is to study and analyze the progress made by Indian banking industry in adoption of technology. The study is secondary based and analytical in nature. The progress in e-banking in Indian banking industry is measured through various parameters such as Computerization of branches, Automated Teller Machines, Transactions through Retail Electronic Payment Methods etc. Statistical and mathematical tools such as simple growth rate, percentages and averages etc are used. The research also highlights the challenges faced by Indian banks in adoption of technology and recommendations are made to tackle these challenges. The research concludes that in years to come e-banking will not only be acceptable mode of banking but preferred mode of banking.

Information Technology has become a necessary tool in today‟s organizations. Banks today operate in a highly globalized, liberalized, privatized and a competitive environment. In order to survive in this environment banks have to use IT. IT has introduced new business paradigm. It is increasingly playing a significant role in improving the services in the banking industry. Indian banking industry has witnessed a tremendous developments due to sweeping changes that are taking place in the information technology.

Electronic banking has emerged from such an innovative development. Modern technology is seen as a panacea for most of the ills that the banking sector faces today. Even at present, India is a relative unbanked country as the credit-to-GDP ratio is one of the lowest in the developing economies. So banks are facing the dual challenge of increasing penetration and high growth trajectory. The banking industry can kill two birds with one stone that is with help of technology. Tremendous progress took place in the field of technology which has reduced the world to a global village and it has brought remarkable changes in the banking industry. Branch banking in the brick and mortar mode has been transformed into click and order channel mode.

E-banking is the term that signifies and encompasses the entire sphere of technology initiatives that have taken place in the banking industry. E-banking is a generic term making use of electronic channels through telephone, mobile phones, internet etc. for delivery of banking services and products. The concept and scope of e-banking is still in the transitional stage. Ebanking has broken the barriers of branch banking.

In India e-banking is of fairly recent origin. The traditional model for banking has been through branch banking. Only in the early 1990s there has been start of non-branch banking services. The good old manual systems on which Indian Banking depended upon for centuries seem to have no place today. The credit of launching internet banking in India goes to ICICI Bank. Citibank and HDFC Bank followed with internet banking services in 1999. Several initiatives have been taken by the Government of India as well as the Reserve Bank to facilitate the development of ebanking in India. The Government of India enacted the IT Act, 2000 with effect from October 17, 2000 which provided legal recognition to electronic transactions and other means of electronic commerce.

The Reserve Bank is monitoring and reviewing the legal and other requirements of e-banking on a continuous basis to ensure that e-banking would develop on sound lines and e-banking related challenges

would not pose a threat to financial stability. A high level Committee under chairmanship of Dr. K.C. Chakrabarty and members from IIT, IIM, IDRBT, Banks and the Reserve Bank prepared the „IT Vision Document- 2011-17", for the Reserve Bank and banks which provides an indicative road map for enhanced usage of IT in the banking sector. To cope with the pressure of growing competition, Indian commercial banks have adopted several initiatives and e-banking is one of them. The competition has been especially tough for the public sector banks, as the newly established private sector and foreign banks are leaders in the adoption of e-banking. Indian banks offer to their customers following e-banking products and services: Automated Teller Machines (ATMs)• Internet Banking• Mobile Banking• Phone Banking• Telebanking.

A mobile phone can be used to communicate with a so-called telephone banker or an automated telephone system, just as well as a fixed line. However, opportunities for mobile phone usage in communication with a bank are much greater. Mobile phone use represents a direct communication channel that spread on a massive scale through which clients have immediate access to typing a bank operation, ordering services or working with accounts.

REVIEW OF RELATED LITERATURE

E-banking may allow banks to offer new products and services, to expand their markets for traditional activities and to consolidate their competitive position in offering available payment services, while ensuring operating costs cut for banks.[1]

The improvement of online banking and its increased use by consumers worldwide has made this service a privileged target for cyber criminals although banks have set up security systems to ensure that transactions conducted online are protected from internet security threats. In fact, electronic banking involves several particular operational risks: one mainly related to the security of systems and transactions, including data confidentiality and authentication of the parties involved, and another concerning the continuous availability of the Internet for financial transactions leading to significant hazards, such as hackers and computer viruses.[2]

Cyber crime, also known as computer crime or electronic crime, is an economic crime committed using computers and the internet. Typical examples of cybercrime are distributing viruses, illegally downloading files, phishing and pharming and stealing personal information such as bank account details.[3]

Phishing and pharming are modern online banking cyber crimes, two of the most organized crimes of the 21st century, representing different ways hackers attempt to manipulate users via the Internet. Phishing is an electronic fraud technique used for financial gain that involves tricking a user into giving confidential personal information, such as passwords, social security numbers, credit card numbers and other personal information.[4]

The number of phishing attacks against banking systems is constantly growing and the methods are constantly evolving. In Japan, for example, phishing scams have targeted bank customers' personal computers via virus, using fake pop-up windows or e-mails masquerading as legitimate internet banking interfaces to trick customers into inputting their personal information.[5]

Pharming is similar to phishing but more sophisticated. It is an electronic fraud technique that allows automatically re-directing a user to a malicious site by modifying DNS entries, which causes users to be directed to a fake version of the web site, identical to the legitimate one, when they try to access their bank's website. In this way, the pharmer is able to capture the personal financial information that the consumer enters into the false web site and the consumer's account is compromised. What makes pharming dangerous is that the attack is unrecognizable to even an alert user. In fact, pharming forces viruses, worms, Trojans and spyware to carry out sophisticated attacks such as hosts file modification, DNS cache poisoning etc.[6]

Regardless of whether one views compulsive buying to be qualitatively or only quantitatively different from normal buying, a good measure of this trait is needed to distinguish compulsive buyers from other members of the population.[7]

This measure should also be able to provide us with an estimate of how common this problem is in the general population. It is, therefore, the purpose of this paper to report our initial efforts at building an effective screening instrument for identifying compulsive buyers and assessing the incidence of compulsive buying within the general population.[8]

OBJECTIVES OF THE STUDY

The objectives of the current research work are as follows:

1. To analyze the future scope of e-banking in India.
2. To study the services of e-banking.

RESEARCH METHODOLOGY

Research is a diligent and systematic inquiry or investigation into a subject in order to discover or receive fact, theories, applications, etc. Methodology is the system of methods followed by particulars discipline. Thus, Research Methodology is the Way how we conduct our research.

This work involves descriptive research design as my project is questionnaire based. Descriptive research includes survey and fact- finding enquiries kinds. The major purpose of descriptive research is description of the state of affairs, as it exists at present.

For this study the sample size is 50 people of the area New Delhi, who were using the E-Banking services.

Bothe primary and secondary date wear used. Primary data were collecting from the questionnaire and rest of the date collecting from the secondary sources like website, Paper, Books and Journals.

ANALYSIS AND INTERPRETATION

The study deals with results which came from the analysis of the primary and secondary data.

In this graph 75% customers are using internet from less than 3 years and 4% are using from 5-10 years and rest of the respondent using internet between the periods of 3-5 year.

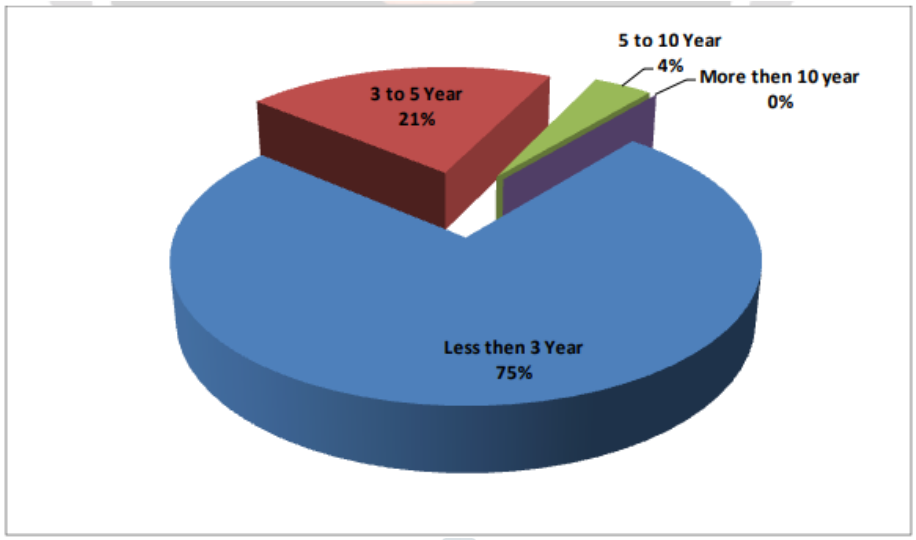

Chart - 1: Internet Using Interval

This study deals with the 77% of male respondent and rest of the respondent is female

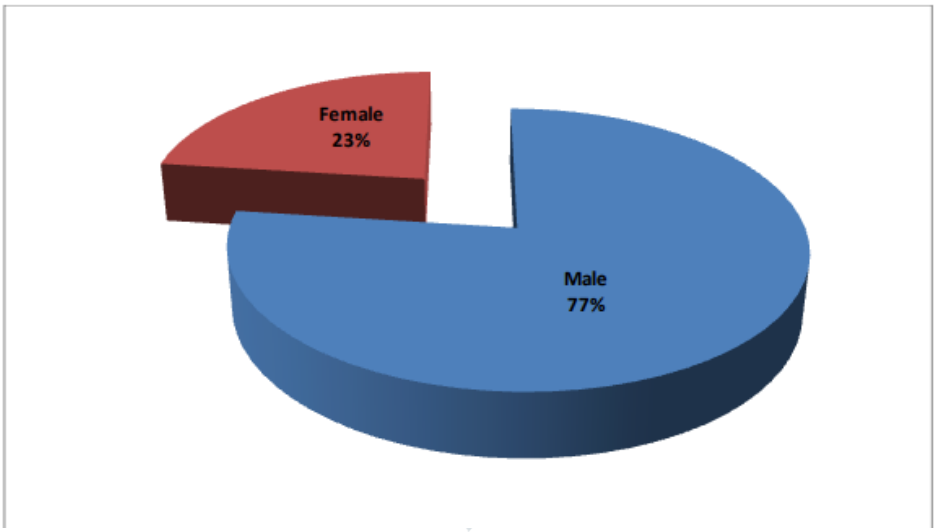

Chart - 2: Gender Ratio

In this graph majority (56%) of the respondent in the age group of 25-30 and 21% are in the group age 30-35 and rest of the age group of 20-25.

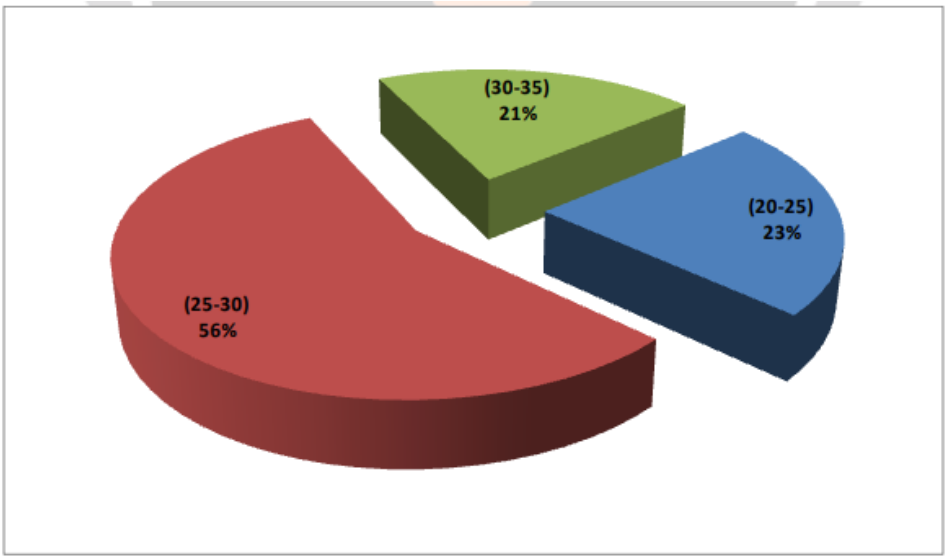

Chart - 3: Age Group

Under the purpose of using internet 42% using for shopping motive and 30% using for entertainment and 6% for research and 19% for banking and 3% other.

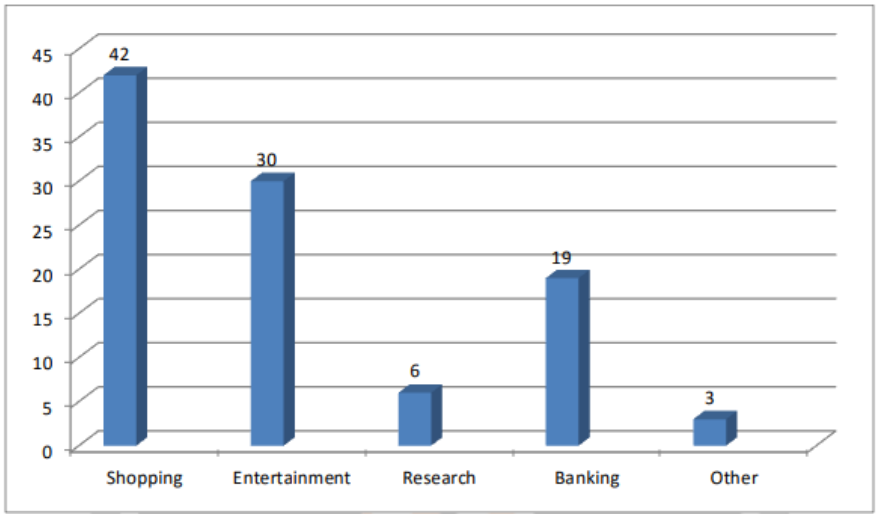

Chart - 4: Objectives

The following graph represents that the majority of respondents are not aware about e-banking (9%) on the other hand 91% respondents know about e-banking.

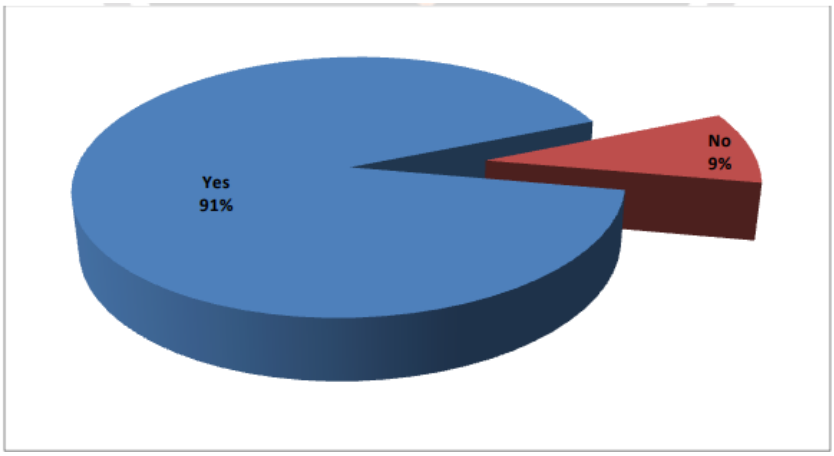

Chart 5: Awareness Level

In this graph 89% respondent using E-banking for their day to day life and the 11% respondent not using the Ebanking.

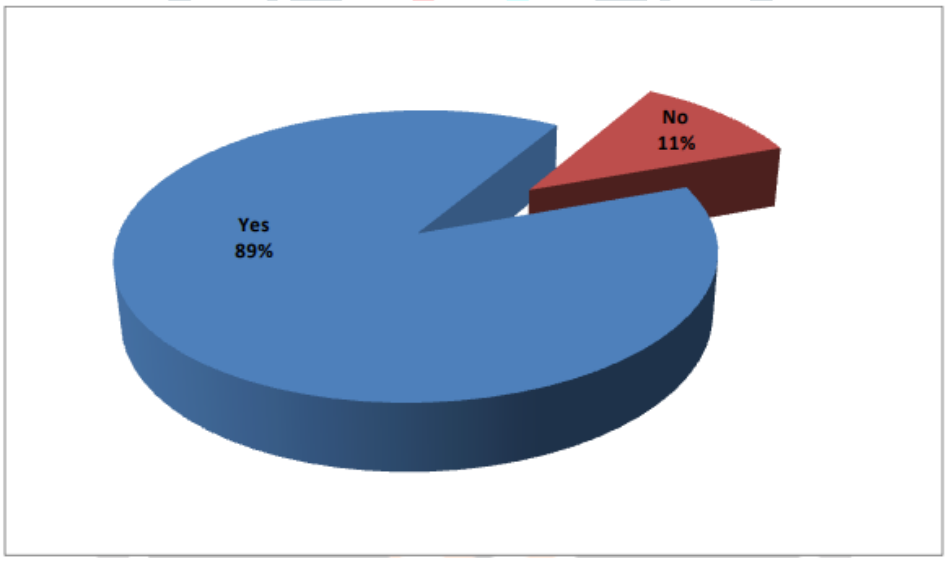

Chart 6: Using the E-Banking

DISCUSSION

SMS banking uses short text messages sent through the client's mobile phone. SMS text messages can be used for both passive and active operations similarly as with classic telephone banking. A client can automatically receive information about his account balance: an SMS is sent to the client immediately after

a certain operation is performed, or on request: a client sends the bank a correctly formatted message which processes it and answers the client's request by SMS.

Information sent on request mostly concerns current interest rates or currency exchange rates. Providing these is simple for the bank because this is publicly accessible information that needs no protection. A client however can request information about the balance in his account, which is not public information and must be protected when it is provided. Passwords are used for this purpose or technologies based on the principle of an electronic key. A client however is required to know the code of every transaction including constant and variable symbols. The whole message containing data separated by # symbols sometimes has up to fifty characters. Users can easily make mistakes. This is frequently a limiting factor for clients, reducing the comfort factor in this service.

The GSM SIM Toolkit service can only be used from a mobile phone supporting this technology. GSM SIM Toolkit is a software interface that enables arbitrary changes to the mobile phone menu. Operators supporting this technology can use it to personalize mobile phone menus. This means that only functions activated and paid for will appear on the user menu. This technology dates back to 1998. Among the first companies to use it in banking applications based on the GSM SIM Toolkit standard were RadioMobil and Expandia Bank in the Czech Republic. Most mobile phones now on the market support for the GSM SIM Toolkit.

To use this service the client needs to be using services of an operator supporting this standard in its network, be a client of a bank that offers handling of accounts through the GSM SIM Toolkit, have a mobile phone supporting GSM SIM Toolkit technology and use a special SIM card for banking services. After buying a special SIM card and activating it at the pertinent bank branch the client can begin using this service.

The mobile phone menu will be widened to include the Banking Services item, through which it is possible to carry out active or passive banking operations. The precise structure differs from one financial institution to another. Security is what is important here. To access banking services it is necessary to know BPUK (PUK for banking applications) and BPIN. BPUK is assigned to a client by the bank when the application is activated and recorded on the mobile phone's SIM card.

BPIN is used for every access to protected items in the banking application. When a client makes three unsuccessful attempts to type the BPIN, access to the banking application and its items is blocked, it is necessary to know the BPUK to unblock it. When the client fails ten times to type the right BPUK the SIM card can no longer be used for banking services. The main advantage of this service is its simplicity. A client just follows instructions on the mobile phone display.

WAP is often compared to web pages, although this is a simplification. Unlike pages appearing on a computer monitor, WAP presents its output on a small mobile phone display, therefore concentrating on text information. It is a form of gateway to various services prepared by a mobile network operator or another firm. One condition for using the service is that the client must have a mobile phone supporting WAP technology. Security is again provided by an electronic key. WAP banking has not caught on very well so far, some banks however continue to offer it despite the relatively low number of users.

Along with significant growth in the usage of mobile phones in banking practice, personal computers have also come to the fore, which to an even greater extent facilitate and modernize banking service provision. In an information society this communication instrument plays an irreplaceable role and is indispensable for the present day banking sphere. The area of electronic banking realized through personal computers can be divided into E-banking, internet banking and mail banking

SIGNIFICANCE OF THE STUDY

E-banking is a service that enables a bank client to handle his accounts from a computer from a place selected in advance, at home or in the office. The main features of E-banking systems are the high level of security, comfort, simplicity of use, openness of the system, wide communication possibilities, networking, definition of users and their rights, automated data transmission and the option to define a combined signature specimen. An E-banking system usually consists of two parts: a bank computer program and a program in the client's computer. The bank program works as a communication server. It receives calls from clients, verifies their identity, receives data from them, authenticates digital signatures, generates digital receipts and sends data to clients.

A E-banking computer system is a multi user application, meaning that several of the client's employees can work with it, in particular: a) administrator – can define new employees, change rights, b) sender – ensures communication with the bank and transmission of prepared data, c) accountant – can type payment orders and orders for collection, b) viewer – can browse through statements and announcements received. This system is open and can be expanded in the future without great cost.

A client cannot avoid visiting the bank though, because he must first ask for an identification code. After opening the bank's web site the client simply selects internet banking and, further to proper identification, can perform passive or active operations. Good internet banking should provide a maximum of services. No less important are the graphic interface, clarity, simplicity, and unambiguity of usage. The intelligibility of texts determines simplicity and speed of understanding of the meaning of menu items, data fields, and general text information displayed to the client. Safety for concrete applications is assured by client authentication, verification of data and data protection by encryption. Client identification is done using passwords or codes. The client chooses some of these and the bank assigns others. It is recommended to choose a password made up of various types of characters, which can be a combination of numbers, lower case and capital letters, and special symbols.

CONCLUSION

Banks usually protect large volume transactions with additional security means, such as an encryption (authentication) calculator, or a token, which generates nonrecurring random passwords, which a client types on confirming an order. The token itself is protected by certain security features. Work with it is only enabled after the client types a four-digit PIN code, whereby the user can change the PIN at any time. In the event of three failed attempts to type the correct PIN the token blocks itself.

After 60 seconds of inactivity a token automatically switches itself off and once switched back on, it again requests the PIN. When a client generates several (for example 10) authentication codes in succession and types none of them into the client system, the key becomes desynchronized. This protection serves to prevent use of the key for other purposes. A cheaper and, based on its dimensions, more practical alternative to a token is a grid card. This is a card with a mesh drawn on it with fields with random generated

characters. The user authorizes an active operation by typing the right code from the field of the card the operator requests from him.

REFERENCES

1. Anwer R., Baig S., Khiyal M.S., Khan A., & Khanum M., (2010-11), 'Online Credit Card Fraud Prevention System for Developing Countries', International Journal of Reviews in Computing, ISSN: 2076-3328, Vol. 2, pp. 62-70.

2. Arias J.C., & Miller R. (2011), 'Market Analysis of Student about Credit Cards', Business Intelligence Journal, Vol. 3, No. 1, pp. 23-36.

3. Berg C., Sanem J., Lust K., Ahluwalia J., Kirch M. & An L., (2010), 'Health-related characteristics and incurring credit card debt as problem behaviors among college students', The Internet Journal of Mental Health, Volume 6, Number 2. ISSN: 1531-2941.

4. Bhatla T.P., Prabhu V., & Dua A., (2013), 'Understanding Credit Card Frauds', Cards Business Review, 01, pp. 01-15.

5. Bhusari V. & Patil S., (2011), 'Study of Hidden Markov Model in Credit Card Fraudulent Detection', International Journal of Computer Applications, Vol. 20, No. 5, pp. 33.

6. Calem P. & Mester L., (2014), 'Consumer Behavior and the Stickiness of Credit Card Interest Rates', The American Economic Review, Vol. 85, No. 5, pp. 1327-1333

7. Chakravorti S., (2013), 'Theory of Credit Card Networks: A Survey of the Literature', Review of Network Economics, Vol. 2, Issue 2, pp. 50-68.

8. Chan P.K., Fan W., Prodromidis A.L. & Stolfo S.J., (2011), 'Distributed Data Mining in Credit Card Fraud Detection', IEEE Intelligent Systems, pp. 67-74.

9. Cumhur E., (2012), 'Factors Affecting the Portability of Credit Card Default and the Intension of Card use in Turkey', International Research Journal of Finance and Economics, Issue 18, ISSN: 1450-2887, pp. 159- 171.

10. Delamaire, Abdou & Pointon, (2011), 'Credit Card Fraud Detection Techniques: A Review', Banks and banks Systems, Vol. 4, Issue 2, pp. 57- 68.

11. Dharwa J.N. & Patel A.R., (2011), 'A Data mining with Hybrid Approach Based Transaction Risk Score Generation Model (TRSGM) for Fraud Detection of Online Financial Transaction', International Journal of Computer Applications, Vol. 6, No. 1, pp. 18-25.

12. Feinberg R.A. (2013), 'Credit Cards as Spending Facilitating Stimuli: A Conditioning Interpretation', Journal of Consumer Research, Vol. 13, No. 3, December.