INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION AND MANAGEMENT

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the area of Computer, Business, Finance, Marketing, Human Resource Management, General Management, Banking, Insurance, Corporate Governance and emerging paradigms in allied subjects like Accounting Education; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Monetary Policy; Portfolio & Security Analysis; Public Policy Economics; Real Estate; Regional Economics; Tax Accounting; Advertising & Promotion Management; Business Education; Business Information Systems (MIS); Business Law, Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labor Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; Public Administration; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism, Hospitality & Leisure; Transportation/Physical Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Digital Logic; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Multimedia; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic and Web Design. The above mentioned tracks are only indicative, and not exhaustive.

Anybody can submit the soft copy of his/her manuscript **anytime** in M.S. Word format after preparing the same as per our submission guidelines duly available on our website under the heading guidelines for submission, at the email addresses: **1** or info@ijrcm.org.in.

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR

IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF _____.**

(e.g. Computer/IT/Engineering/Finance/Marketing/HRM/General Management/other, please specify).

DEAR SIR/MADAM

Please find my submission of manuscript titled '_____' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication anywhere.

I affirm that all author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR:

Designation:

Affiliation with full address, contact numbers & Pin Code:

Residential address with Pin Code:

Mobile Number (s):

Landline Number (s):

E-mail Address:

Alternate E-mail Address:

2. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS:** The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT:** Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS:** Abstract must be followed by list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.

6. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of the every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.

7. **HEADINGS:** All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

8. **SUB-HEADINGS:** All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

9. **MAIN TEXT:** The main text should follow the following sequence:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESES

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

SCOPE FOR FURTHER RESEARCH

ACKNOWLEDGMENTS

REFERENCES

APPENDIX/ANNEXURE

It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed 5000 words.

10. **FIGURES &TABLES:** These should be simple, centered, separately numbered & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. It should be ensured that the tables/figures are referred to from the main text.

11. **EQUATIONS:** These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.

12. **REFERENCES:** The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio," Ohio State University.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITE

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on December 17, 2011 http://epw.in/user/viewabstract.jsp

MODERN FACES OF FINANCIAL CRIMES IN ELECTRONIC BANKING SYSTEM

VIKAS SHARMA
INCHARGE
COMPUTER CENTRE
INTERNATIONAL CENTRE FOR DISTANCE EDUCATION AND OPEN LEARNING
HIMACHAL PRADESH UNIVERSITY
SHIMLA

ABSTRACT

The globalisation and liberalization of Indian Economy during 90s has forced the traditional Indian Banks to change their legacy face with deployment of numerous Information Technology enabled banking products and service delivery channels. For banks, the electronic banking (eBanking) is consolidation and accessibility of transactional database at a central location but for general customers; it is accessibility of banking services at their doorstep, 24 hrs a day and 7 days in a week. This paper discusses that the increasing dependence on Information Technology has significantly enhanced the risks of financial crimes (FCs) in addition to the traditional ones. The FCs include unauthorised access and alteration of information, changing of information path in middle way, cheating, frauds, money laundering, virus attacks, denial of services, email threats, etc. There is a need to deploy secure computing and communication infrastructure, controlled accessibility, maintaining of confidentiality & integrity of customers' information against unauthorised usage within the internal as well as external network environment as well as to enhance awareness among customers for safe and secure eBanking.

KEYWORDS
Denial of Service, Financial Crimes, Hacking, Information and Communication Technology, PKI, Viruses, Worm.

INTRODUCTION

The banks play very vital role for development of any nation. The bank is a financial organisation that controls, influences and manages finance, which in turn facilitate in development of nation's economy. It provides an environment that is helpful for the social and economic development of the nation (Sharma, 2008). The globalisation of Indian Economy has forced the Indian Banks to equip themselves with modern banking technologies to compete in the domestic as well in the international level market. The Information and Communication Technology has become the state-of-the-art technology for the banks to manage their resources, reduce operational cost, enhance efficiency and productivity and provide banking services to their customers at their doorsteps, 24 hrs in day and 7 days a week. To meet the current challenges of this open economy, the banks have been preparing themselves to harness the opportunities that globalisation and financial liberalisation provided through extensive use of IT (RBI, 1999). But ICT is also like a naked wire where majority of banks all over the world have been struggling to protect their valuable assets i.e. information from the internal as well as external threats. Internet being a public network has been in use by the banks for flow of data / information. This is also the channel used by the unauthorised persons to get admission, alter and damage data (RBI, 2005). The banks as a finance-dealing agency attract many intruders internally as well as externally to commit frauds. These persons generally shift the actual route of information (data/information) flow and get unauthorized access to commit huge financial loss to the organisation. Thus, access control is of paramount importance in banking environment. Attackers could be hackers, unscrupulous vendors, disgruntled employees or even pure thrill seekers. It is therefore, necessary that banks should have secure access control measures in place to avoid any unpleasant incident (RBI, 2005). In addition to external attacks, the banks are exposed to security risk from internal sources e.g. frauds by employee. Employees being familiar with different systems and their weaknesses are potential security threats in a loosely controlled environment (RBI, 2005). Many banks have tied up with outside service providers to implement, operate and maintain their eBanking systems because these don't have expertise. This adds the operational as well as security risks. The over dependencies on third parties/vendors should be avoided as far as possible (RBI, 2005).

FINANCIAL INFORMATION SECURITY- A CHALLENGE

The characteristics of computer crime are different from that of conventional crime in that it is relatively easy to commit, difficult to detect and even harder to prove. It is a 'low risk, high reward' venture for the criminals (Talwar, 1999**).** The computers are able to store huge volume of data in small space. It is difficult to transfer one lac rupees physically from a bank's vault than to transfer digital information on money by breaking into the bank's server (Delhi Police, "Cyber Crimes", 2003). In the financial service industry alone, the spending on security related products and service was expected to rise from $ 848 million in 2000 to 2.2 billion by 2005. Thus, there is a sizable requirement of cyber security products and services (CEDTI, 2005). In India, the spending by companies on Information Security ranges from 5% to 15% of the IT budget (Gupta, et. al., 2004). In cyberspace, there is no policemen to patrol/monitor the information superhighway, leaving it open to everyone (Vaidya-Kapoor, 2004). The criminals find banks to be a profitable target. Nearly 39 per cent of cyber crime cases in India are related to banks and Financial Institutions excluding those of the government (O'BRIEN, 2003). In 66 % cases of data theft employees or former employees were evolved. The employees are reported as the one of the biggest vulnerable of security elapses (ASCL, 2003). With the growing popularity of ATMs, Debit, Credit Cards and Internet Banking in India, the customers have been becoming the maximum victims of cyber crimes. Plastic cards have given rise to frauds such as alteration of signature on the cards, forgery of signature to match the signature on the card, collusion with retailers using genuine cards, counterfeit of entire cards, etc. (Hussain, 1988). A survey from Gartner Banks reveal that banks lost over USD 2 billion to fraudsters in the year 2003, with nearly 2 million Americans had been losing funds from their cheque accounts at an average of USD 1,200 per incident (ePaynews, "Accounts Robbed", 2004). The ongoing investigations in Southwest Florida revealed biggest-yet credit card fraud ring. The identities of up to 1,400 individuals have been stolen, although not all were used to make false credit cards (ePaynews, "Stole Identities", 2004). Similarly in New York, Credit Cards holders' data was stolen from clothing retailer the Polo Ralph Lauren Corp. This incident forced the banks and credit cards issuers to warn thousand of consumers that their credit-card information might have been exposed and needed to be replaced immediately. This incident affected almost 180,000 card holders (Associated Press, 2005) Earlier, the London-based Reed Elsevier Group PLC, which owns LexisNexis, disclosed that criminals might have breached computer files containing the personal information of 310,000 people since January 2003 (Associated Press, 2005). Instead of using ICT for the well beings of society and the national development, it is being in use to do cyber crimes, defaming persons and anti national activities.

CATEGORIES OF FINANCIAL CRIMES

The Information Technology has been in use to commit Financial Crimes (FCs). The FCs include unauthorised access and alteration of information, changing of information path in middle way, cheating, frauds, money laundering, virus attacks, denial of services, email threats, etc. The financial crimes can be committed in numerous following forms.

HACKING

This is unauthorized access to computer systems or networks. It is a kind of access without the permission of rightful owner or the person in charge of computer. In other words it is a criminal activity to enter into the territory of third party without its permission or desire and gain access of computer resources. Here are

some types of unauthorized access (Delhi Police, "Cyber Crimes", 2003): a) Packet Sniffing is a technology used by the crackers to get in the access of information that is being transferred during communication by two parties. It is used to check the messages that are being transmitted in the form of small packets during transmission. b) Tempest Attack is a technique to monitor electromagnetic emissions from computers in order to reconstruct the data. This allows remote monitoring of network cables or remotely viewing monitors. c) Password Cracking is a technique used by the hacker to gain access to the systems by using Password Cracking utilities**.** d) Buffer Overflow is probably the most common way of breaking into the computer. It involves input of excessive data into a computer. The excess data "overflows" into other areas of the computer's memory. This allows the hacker to insert executable code along with the input, thus enabling the hacker to break into the computer.

DATA THEFT

This includes theft of information stored in computer hard disks, removable storage media, etc. Here are few cases of data theft incidents occurred in India (O'BRIEN, 2003):

- An employee of the Bank of India trapped his organisation's computer network and gathered data on all keys pressed, including passwords, by monitoring the CCTV.
- GS Bhatnagar, a resident of South Delhi, realised that Rs 10,000 had been withdraw from his account at SBI through his ATM card. This happened, when Bhatnagar had never used his card in any banking operation.
- A MBA graduate Akaash Singh hacked into an ATM while using a metallic sleeve to wash up several lakhs of cash from a Canara Bank Branch in Chennai. The first data theft (credit card information) case registered in India in 2002, in which a person Arif Azim, who had been working at a call centre in Nodia gained access to a credit card number of an American National while performing his official duties (Kaur, 2004).

SALAMI ATTACKS

An employee of a bank in USA was dismissed from his job. Disgruntled at having been mistreated by his employer the man first introduced a logic bomb (LB) into the bank's systems. The LB is a computer programme that activates on the occurrence of a particular predefined event. The logic bomb was programmed in such a way to take ten cents from all the accounts in the bank and put them into the account of the person whose name was alphabetically the last in the bank's rosters on every Saturday. The disgruntle employee opened an account in the bank with name of Ziegler. The withdrawn amount was so insignificant that neither any of the account holders nor the bank officials noticed the fault. It was brought to their notice when a person by the name of Zygler opened his account in that bank. He was surprised to find a sizable amount of money being transferred into his account on every Saturday. This was because; his name (Zygler) came to the last in bank's rosters instead of Ziegler (Delhi Police, "Cyber Crimes", 2003).

DENIAL OF SERVICE ATTACK

Denial-of-service (DoS) attacks are usually launched to make a particular service unavailable to someone who is authorized to use it. These attacks may be launched using one single computer or many computers across the world. In the latter scenario, the attack is known as a distributed denial of service attack. Denial-of-Service tools allow the attackers to automate and preset the times and frequencies of such attacks so that the attack is launched and then stopped to be launched once again later. This makes it very difficult, in fact almost impossible, to trace the source of the attack. The above tools also facilitate the hackers to automatically change the source addresses of the systems randomly, thereby making it seem as if the attack is originating from many thousands of computers while in reality there may be only a few. The victims of such types of attack have been like the Amazon, CNN, Yahoo and eBay etc. (Delhi Police, DOS, 2003).

VIRUS ATTACKS

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. The Virus can cause severe damage to the victim's assets- "the information" (ASCL, 2003). The VBS_LOVELETTER virus (better known as the Love Bug or the I LOVE YOU virus) was reportedly written by a Filipino undergraduate student. In May 2000, the Melissa virus became the world's most prevalent virus. It corrupted one in every five personal computers in the world. The Losses incurred during this virus attack were pegged at US $ 10 billion (Delhi Police, "Cyber Crimes", 2003). "I LOVEYOU" virus created havoc in the United States after crippling government and business computers in Asia and Europe. The victim organisations were American State Department, CIA and major companies like Ford and Time-Warner. Love Bug e-mail appeared on computer screens in both houses of Congress in the Washington, the White House, the FBI and at the Pentagon. Trend Micro, a Computer security firm says that some 1.27 million computer files were infected worldwide, with nearly 1m in the US. Experts say the Love Bug is much more serious than Melissa as it overwrites audio and picture files, replacing them with its own code. The virus is reactivated if one of these files is subsequently opened (Delhi Police, **"**'Viruses", 2003). Viruses are very dangerous; they spread faster than they are stopped.

WORMS

These are malicious codes just like Viruses. But, unlike Viruses they do not need the host to attach themselves. They travel through holes in the network i.e. open/ unguarded ports. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory (Delhi Police, "Cyber Crimes", 2003).

TROJANS

These are unauthorized programs which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing. It installs client-server architecture on the victim's and hacker's computers respectively and the hacker gains full control of the victim's computer. A report on a website owned by Consumers' Institute of New Zealand, Inc., says a man from Auckland had his bank account robbed through the Internet in April 2004. The $20,000 was transferred from his BNZ business account to a bank in Estonia. This transfer reportedly happened at 7.30 pm and was cleared and gone by midnight. On inquiry, it found that victim's laptop was infected by a Trojan Horse program. The program may have come in as an email attachment or website advertisement. The program read the keystrokes, which were recorded and transmitted back to the fraudsters, giving them access to conduct online banking transaction (Infotech, 2004).

WEB JACKING

It is a type of cyber crime where someone forcefully takes control of a website by cracking its administrative password and later changing it. The actual owner of the website does not have any more control over it. The hacker changes the contents of web site as per his interests and demands ransom in huge amount of money. In a recent incident in USA where the owner of a hobby website for children received an e-mail informing her that a group of hackers had gained control over her website. They demanded a ransom of 1 million dollars from her. (Delhi Police, "Cyber Crimes", 2003).

E-MAIL RELATED ATTACKS

Email has fast emerged as the world's most preferred form of communication. Billions of email messages traverse the globe daily. Email is also misused by criminal elements. Some of the major email related crimes are: a) Email Spoofing, b) Sending Malicious Codes through email, c) Email Bombing, d) Sending Threatening emails, e) Defamatory emails, and f) Email Frauds (Delhi Police, 'e-mail", 2003).

- A spoofed email is one that appears to originate from one source but has actually emerged from another source. Falsifying the name and/or email address of the originator of the email usually does email spoofing. The criminal can send viruses, Trojans, worms etc to victims system who in turn at the other end can open it by trusting that the sender is the original creator of the message. Email spoofing is very often used to commit financial crimes. In a recently reported case, a Pune based businessman received an email from the Vice President of the Asia Development Bank (ADB) offering him a lucrative contract in return for Rs 10 lakh. The businessman verified the email address of the Vice President from the web site of the ADB and subsequently transferred the money to the bank account mentioned in the email. It later turned out that the email was a spoofed one and was actually sent by an Indian based in Nigeria.
- Email is in use to propagate malicious code over the Internet. The Love Bug virus, for instance, reached millions of computers within 36 hours of its release from the Philippines. Hackers often attach Trojans, viruses, worms and other computer contaminants with e-greeting cards. Sometimes the computer

contaminants may contain software that appears to be an anti-virus patches. The victim downloads these by trusting that it is an anti virus software etc. but in originality, it is malicious code.

– Email bombing is a process to send a large amount of emails to the victim's system which may result in crashing. It is due to intentionally subscribing the victim's email address to a large number of mailing lists. The mailing lists generates lots of messages daily which inturn increase large traffic to victims account and it may full. The service provider will probably delete his/her account (Delhi Police, "Cyber Crimes", 2003).

CONCLUSION AND RECOMMENDATIONS

The deployments of eBanking solutions have enhanced the overall financial crime profile of banks in addition to the traditional crimes. It is the responsibility of the bank management to analyse not only the traditional risks but also the newly emerged risks. It is very difficult to achieve absolute security in this vulnerable digital world. To protect our banks against financial crimes, there are only two options- either shut down all doors from outer world or implement strong security controls. No doubt, the first option may provide us hundred percent secure environment but the biggest question is "Can we survive like this?" Certainly the answer is "no" because we are living in an open world economy and applications of ICT are just like veins to carry blood in present banking system. So there is a need to implement safe and sound infrastructure, security policies and their periodic review to check for vulnerabilities. The safe and sound infrastructure includes deployment of firewalls, instruction detection systems (IDS), limited access rights to the employees/customers, public key infrastructure, digital signatures, etc. Incidents of data thefts, unauthorized data alteration, unauthorized access, etc. can be mitigated by proper use of Public Key Infrastructure (PKI) and Digital Signatures. The PKI is also helpful to maintain integrity, confidentiality and non-repudiation of message. To meet the internal security threats within the organisation, there is a need to provide limited accesses to the users, segregation of their roles and duties, etc.

REFERENCES

1. ASCL (2003): Computer Crime & Abuse Report (India) 2001-02. Asian School of Cyber Law. Viewed on 28 Sept. 2011. http://www.asianlaws.org/report0102.pdf
2. Associated Press (2005): Security breach puts thousands of credit card holders at risk. Viewed on 02 May 2011. http://www.stltoday.com/stltoday/business/stories.nsf/story/ B5078866F26C382286256FE40007D7F7?OpenDocument
3. CEDTI (2005): Secure Your Business through Information Security. Feb 2005. Centre For Electronics Design & Technology of India, Mohali. Viewed on 03 May 2005. http://www.cedtimohali.org/workshop/index.htm
4. Delhi Police (2003): Computer Virus. Cyber Cell Crime Branch. Viewed on 10 Oct. 2010. http://cybercrime.planetindia.net/index.htm
5. ---. Denial of Services. 2003. Cyber Cell Crime Branch. Viewed on 10 Oct. 2010. http://cybercrime.planetindia.net/index.htm
6. ---.eMail Crimes. 2003. Cyber Cell Crime Branch. Viewed on 10 Oct. 2010. http://cybercrime.planetindia.net/index.htm
7. ---.Frequently Used Cyber Crimes. 2003. Cyber Cell Crime Branch. Viewed on 10 Oct. 2010. http://cybercrime.planetindia.net/index.htm
8. ePaynews (2004): Florida Cartel Stole Identities of 1,100 Cardholders. 15 Jun 2004. Viewed on 02 May 2005. http://www.epaynews.com
9. ePaynews (2004): Two Million Bank Accounts Robbed In Past Year. Jun 15 2004. Viewed on 02 May 2005. http://www.epaynews.com
10. Gupta Ashish, et. al (2004): Information Security Environment in India. NASSCOM- Evalueserve. Viewed on 24 Sept. 2004. http://www.nasscom.org/download/NASSCOM-EVS%20Report%20on%20Information%20Security%20Environment%20in%20India.pdf
11. Husain Farhat (ed.), (1988). Introduction. Computerisation and Mechanisation in Indian Banks, Deep & Deep Publication, New Delhi.
12. IDRBT (2003): FAQ. Institute for Development and Research in Banking Technology Hyderabad. Viewed on 19 Jan. 2005. http://idrbtca.org.in/
13. Infotech (2004): Viewed on 21 Apr. 2005. http://infotech.indiatimes.com/articleshow/762313.cms
14. Kaur Jasmine (2004): Red Alert, Netizens!. Data Quest. Viewed on 7 Oct. 2004. http://www.dqindia.com/content/enterprise/2004/104091401.asp
15. O'BRIEN, ALLEN (2003): Innovation time for India's cyber crime. Viewed on 15 Oct. 2004. http://cybercrime.planetindia.net/innovation_time.htm
16. RBI (2005): Report on Internet Banking. Reserve Bank of India. Viewed on 17 Feb. 2005. http://www.rbi.org.in/sec21/21595.pdf
17. ---.IT and the Banking Sector. Reserve Bank of India. Viewed on 31 Dec. 2004. http://www.rbi.org.in/index.dll/7970?OpenStoryTextArea?fromdate=11/28/96& todate=11/16/04&
18. Sharma Vikas (2008): "Progress, Trends and Management in e-Banking: A Case Study of Banks in Himachal Pradesh". Thesis. Institute of Management Studies. Himachal Pradesh University, Shimla. 2008
19. Talwar S. P. (1999): Computer Related Crime." Inaugural Address at the National Seminar on Computer Related Crime by Deputy Governor. Reserve Bank of India at New Delhi. Viewed on 31 Dec. 2010. http://www.rbi.org.in/index.dll/5324?OpenStory TextArea? fromdate=11/28/96&todate=11/16/04&
20. Vaidya-Kapoor, Gopika (2004): Byte by Byte. 18 Feb. 2003. Rediff.com. Viewed on 25 Sept. 2011. http://www.rediff.com/netguide/2003/feb/18crime.htm

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application and Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mails i.e. **infoijrcm@gmail.com** or **info@ijrcm.org.in** for further improvements in the interest of research.

If you have any queries please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-

Co-ordinator