

INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT

I
J
R
C
M



A Monthly Double-Blind Peer Reviewed Refereed Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.

as well as in Open J-Gate, India [link of the same is duly available at infibnet of University Grants Commission (U.G.C.)]

Registered & Listed at: Index Copernicus Publishers Panel, Poland

Circulated all over the world & Google has verified that scholars of more than 1500 Cities in 141 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

www.ijrcm.org.in

CONTENTS

Sr. No.	TITLE & NAME OF THE AUTHOR (S)	Page No.
1.	ANALYSIS OF IPOs UNDERPRICING: EVIDENCE FROM BOMBAY STOCK EXCHANGE ROHIT BANSAL & DR. ASHU KHANNA	1
2.	BANKRUPTCY PREDICTION OF FIRMS USING THE DATA MINING METHOD ATIYE ASLANI KTULI & MANSOUR GARKAZ	8
3.	THE EFFECT OF BASEL III REQUIREMENTS ON IMPROVING RISK-MANAGEMENT CAPABILITIES IN JORDANIAN BANKS DR. MOHAMMED FAWZI ABU EL HAJJA	12
4.	CAPITAL STRUCTURE DETERMINANTS: CRITICAL REVIEW FOR SELECTED INDIAN COMPANIES DR. AVANISH KUMAR SHUKLA	18
5.	IMPACT OF INFLATION ON BANK LENDING RATE IN BANGLADESH EMON KALYAN CHOWDHURY	23
6.	THE PERCEPTION OF BANK EMPLOYEES TOWARDS COST OF ADOPTION, RISK OF INNOVATION, AND STAFF TRAINING'S INFLUENCE ON THE ADOPTION OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) IN THE RWANDAN COMMERCIAL BANKS MACHOGU MORONGE ABIUD & LYNET OKIKO	27
7.	ICT, ELECTION AND DEVELOPMENT IN AFRICA NDUONOFIT, LARRY-LOVE EFFIONG & ONWUKWE, VIVIAN CHIZOMA	32
8.	MODERATING ROLE OF EMOTIONAL INTELLIGENCE TOWARDS STRESS AND EMPLOYEE PERFORMANCE IN THE INDIAN BANKING SECTOR BEULAH VIJI CHRISTIANA.M & DR. V. MAHALAKSHMI	35
9.	FACTORS INFLUENCING CUSTOMER LOYALTY IN MOBILE PHONE SERVICE - A STUDY WITH REFERENCE TO COIMBATORE CITY DR. V.T.R .VIJAYAKUMAR & B.SUBHA	39
10.	A STUDY ON OCCUPATIONAL STRESS AMONG GRADE I POLICE CONSTABLES M.SHUNMUGA SUNDARAM & DR. M. JAYA KUMARAN	44
11.	A STUDY ON THE IMPACT OF SPIRITUALITY ON ORGANISATIONAL PERFORMANCE WITH SPECIAL REFERENCE TO ORGANISATIONS IN SALEM CITY DR. M. G.SARAVANA RAJ & R. FLORENCE BHARATHI	49
12.	A COMPARATIVE STUDY OF SELF- EFFICACY AND SUBJECTIVE WELL- BEING AMONG EMPLOYED WOMEN AND UNEMPLOYED WOMEN DR. K. JAYASHANKAR REDDY	54
13.	NETWORK SECURITY THREATS AND SOLUTIONS IN A VIRTUAL MARKETPLACE DR. PANKAJ KUMAR GUPTA & DR. AJAY KUMAR TIWARI	58
14.	A STUDY OF SUPPLIERS CERTIFICATION AT DIFFERENT LAYERS AND ITS IMPACT ON QUALITY IN AUTO COMPONENT INDUSTRY DR.DATTATRY RAMCHANDRA MANE	61
15.	GLOBAL LIFE INSURANCE PENETRATION AND DENSITY DR. GUDALA SYAMALA RAO	69
16.	AN ENHANCE SECURITY OF PLAYFAIR CIPHER SUBSTITUTION USING A SIMPLE COLUMNAR TRANSPOSITION TECHNIQUE WITH MULTIPLE ROUNDS (SCTTMR) GAURAV SHRIVASTAVA, MANOJ DHAWAN & MANOJ CHOUHAN	75
17.	CONSUMERS PERCEPTIONS OF CORPORATE SOCIAL RESPONSIBILITY: EMPIRICAL EVIDENCE AMIT B. PATEL, DR. VIMAL K. BHATT & JATIN K. MODI	79
18.	A STUDY ON FINANCIAL HEALTH OF KINGFISHER AIRLINES LTD: (Z- SCORE APPROACH) JIGNESH. B. TOGADIYA & UTKARSH. H. TRIVEDI	84
19.	STRATEGIES OF CUSTOMER RELATION MANAGEMENT IN MODERN MARKETING DR. T. PALANISAMY & K. AMUTHA	88
20.	CORPORATE GOVERNANCE IN OIL & GAS SECTOR: AN EMPIRICAL INVESTIGATION RASHESH PATEL & SWATI PATEL	92
21.	KNOWLEDGE MANAGEMENT & MOBILIZING KNOWLEDGE IN EDUCATION BY FOLLOWING CASE STUDY OF YU;GI-OH WORLD SMITA.SJAPE	101
22.	STUDY OF CRM THROUGH SOCIAL NETWORKING SITE: A FACEBOOK PERSPECTIVE TEENA BAGGA & APARAJITA BANERJEE	107
23.	ORDINARY LEAST SQUARES METHOD AND ITS VARIANTS R. SINGH	114
24.	IT INFRASTRUCTURE IN CREATING POTENTIAL MARKETING OPPORTUNITIES IN INDUSTRIES: AN EMPIRICAL STUDY OF SELECT INDUSTRIES IN KARNATAKA MANJUNATH K R & RAJENDRA M	120
25.	THE IMPACT OF KNOWLEDGE MANAGEMENT ON BUSINESS ORGANIZATION SUNITA S. PADMANNAVAR & SMITA B. HANJE	126
26.	LOCUS OF CONTROL AMONG HIGH SCHOOL TEACHERS DEEPA MARINA RASQUINHA	129
27.	KNOWLEDGE MANAGEMENT: A CONCEPTUAL UNDERSTANDING AINARY ARUN KUMAR	135
28.	A STUDY ON EFFECTIVENESS OF ORGANIZATIONAL HEALTH IN SMALL SCALE INDUSTRIES DR. J. S. V. GOPALA SARMA	142
29.	JOB SATISFACTION DURING RECESSION PERIOD: A CASE STUDY OF PUBLIC & PRIVATE INSURANCE IN PUNJAB HARDEEP KAUR	149
30.	BANKING SECTOR REFORMS IN INDIA DR. SANDEEP KAUR	156
	REQUEST FOR FEEDBACK	162

CHIEF PATRON

PROF. K. K. AGGARWAL

Chancellor, Lingaya's University, Delhi
Founder Vice-Chancellor, Guru Gobind Singh Indraprastha University, Delhi
Ex. Pro Vice-Chancellor, Guru Jambheshwar University, Hisar

PATRON

SH. RAM BHAJAN AGGARWAL

Ex. State Minister for Home & Tourism, Government of Haryana
Vice-President, Dadri Education Society, Charkhi Dadri
President, Chinar Syntex Ltd. (Textile Mills), Bhiwani

CO-ORDINATOR

AMITA

Faculty, Government M. S., Mohali

ADVISORS

DR. PRIYA RANJAN TRIVEDI

Chancellor, The Global Open University, Nagaland

PROF. M. S. SENAM RAJU

Director A. C. D., School of Management Studies, I.G.N.O.U., New Delhi

PROF. M. N. SHARMA

Chairman, M.B.A., Haryana College of Technology & Management, Kaithal

PROF. S. L. MAHANDRU

Principal (Retd.), Maharaja Agrasen College, Jagadhri

EDITOR

PROF. R. K. SHARMA

Professor, Bharti Vidyapeeth University Institute of Management & Research, New Delhi

CO-EDITOR

DR. BHAVET

Faculty, M. M. Institute of Management, Maharishi Markandeshwar University, Mullana, Ambala, Haryana

EDITORIAL ADVISORY BOARD

DR. RAJESH MODI

Faculty, Yanbu Industrial College, Kingdom of Saudi Arabia

PROF. SANJIV MITTAL

University School of Management Studies, Guru Gobind Singh I. P. University, Delhi

PROF. ANIL K. SAINI

Chairperson (CRC), Guru Gobind Singh I. P. University, Delhi

DR. SAMBHAVNA

Faculty, I.I.T.M., Delhi

DR. MOHENDER KUMAR GUPTA

Associate Professor, P. J. L. N. Government College, Faridabad

DR. SHIVAKUMAR DEENE

Asst. Professor, Dept. of Commerce, School of Business Studies, Central University of Karnataka, Gulbarga

MOHITA

Faculty, Yamuna Institute of Engineering & Technology, Village Gadholi, P. O. Gadholi, Yamunanagar

ASSOCIATE EDITORS

PROF. NAWAB ALI KHAN

Department of Commerce, Aligarh Muslim University, Aligarh, U.P.

PROF. ABHAY BANSAL

Head, Department of Information Technology, Amity School of Engineering & Technology, Amity University, Noida

PROF. A. SURYANARAYANA

Department of Business Management, Osmania University, Hyderabad

DR. SAMBHAV GARG

Faculty, M. M. Institute of Management, Maharishi Markandeshwar University, Mullana, Ambala, Haryana

PROF. V. SELVAM

SSL, VIT University, Vellore

DR. PARDEEP AHLAWAT

Associate Professor, Institute of Management Studies & Research, Maharshi Dayanand University, Rohtak

DR. S. TABASSUM SULTANA

Associate Professor, Department of Business Management, Matrusri Institute of P.G. Studies, Hyderabad

SURJEET SINGH

Asst. Professor, Department of Computer Science, G. M. N. (P.G.) College, Ambala Cantt.

TECHNICAL ADVISOR

AMITA

Faculty, Government H. S., Mohali

MOHITA

Faculty, Yamuna Institute of Engineering & Technology, Village Gadholi, P. O. Gadholi, Yamunanagar

FINANCIAL ADVISORS

DICKIN GOYAL

Advocate & Tax Adviser, Panchkula

NEENA

Investment Consultant, Chambaghat, Solan, Himachal Pradesh

LEGAL ADVISORS

JITENDER S. CHAHAL

Advocate, Punjab & Haryana High Court, Chandigarh U.T.

CHANDER BHUSHAN SHARMA

Advocate & Consultant, District Courts, Yamunanagar at Jagadhri

SUPERINTENDENT

SURENDER KUMAR POONIA

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; Management 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 address: infoijrcm@gmail.com.

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR
IJRCM

Subject: SUBMISSION OF MANUSCRIPT IN THE AREA OF _____.

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

DEAR SIR/MADAM

Please find my submission of manuscript entitled ' _____ ' 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 elsewhere.

I affirm that all the 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 the 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:

NOTES:

- a) The whole manuscript is required to be in **ONE MS WORD FILE** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
- b) The sender is required to mention the following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)
- c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
- d) The total size of the file containing the manuscript is required to be below **500 KB**.
- e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
- f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

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 a 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 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, crystal clear, 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 the 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, Nigeria.

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.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 <http://epw.in/user/viewabstract.jsp>

NETWORK SECURITY THREATS AND SOLUTIONS IN A VIRTUAL MARKETPLACE

DR. PANKAJ KUMAR GUPTA
ASSOCIATE PROFESSOR
DEPARTMENT OF IT & MANAGEMENT
TIRUPATI COLLEGE OF TECHNICAL EDUCATION
JAIPUR

DR. AJAY KUMAR TIWARI
ASSOCIATE PROFESSOR
DEPARTMENT OF IT & MANAGEMENT
TIRUPATI COLLEGE OF TECHNICAL EDUCATION
JAIPUR

ABSTRACT

Network security problems are assorted and can variously affect the assets in a Virtual Marketplace. The solution to these problems has to be based on both technology and legislation. In this paper, in this paper we focus on those security threats with partial or full technological solution. We look at some of the new technologies that can change or have already changed the level of security in the global network, and some prospects for the future. This paper discusses our view of the assets that require protection in a Virtual Marketplace, the potential sources of threat, and the likely methods of attack. We then examine various types of security threats, including some "cutting edge" technology solutions, and explore how digital enterprises can be managed (and are being managed) more securely using these technology solutions.

KEYWORDS

E-Commerce Security, Network Security, Internet Security, Security Solutions.

INTRODUCTION

In order for virtual marketing to succeed, customers must have confidence in the transmission of sensitive financial and personal information across networks to designated business organizations; digital enterprises must be certain in the knowledge that information collected over web storefronts is indeed valid; and furthermore, businesses must undertake additional precautions to ensure that databases with confidential information from their customers are not compromised by hackers or malicious employees. The solution to these problems has to be based on both technology and legislation. In this paper, we focus on the new technologies that can change or have already changed the level of security in the global network.

NETWORK ASSETS

The following are assets of e-commerce and other network based services, which require protection in a Virtual Marketplace:-

- The personal data supplied by consumers need to be protected while in transit, while stored in company files and databases, and in future use. They must be protected against loss, damage, unwarranted changes and unwarranted third party disclosures.
- The corporate databases of the organization offering goods and services by e-commerce must be protected as in a.
- The applications and delivery platforms of the organization offering goods and services by e-commerce must be protected against all threats to its availability and integrity of its services.
- Payment-related records and other records of value must be protected at a higher level than other customer data against fraud and privacy abuses.

POTENTIAL SOURCES OF THREAT

We can broadly classify sources of threat into the following two categories.

- 1) **Outside Individuals and Organizations:** This includes competitors in the market place, individuals and groups with a strong motivation to disrupt the services or gather intelligence, either for personal gain or other reasons. Competing organizations may be also lured by information about customers, debtors and suppliers besides strategic plans of the company. Certain outside organizations and individuals may be criminal or terrorist organizations or their representatives looking for opportunities to create fraud or disrupt or bring down e-commerce services.
- 2) **Legitimate Users, Business Associates and Employees:** These individuals may unintentionally damage e-commerce services or cause disruption to them sometimes as a result of mistakes, other times due to poor training, yet other times due to security breaches caused by them. In most of these cases, violations may be traced to the individual concerned and corrective actions such as sanctions and additional training are possible.

METHODS OF ATTACK

The following are the major types of attacks.

- **Unauthorized Access:** This means accessing or misusing a computer system to intercept transmissions and steal sensitive information. This may be from an external source or by an insider acting on behalf of a hostile organization or for self-interest.
- **Service Denial:** This means that an attacker shuts down your site or denies access to visitors. This is done by overloading the system with excessive numbers of requests for service. This may also be done by the use of malicious software such as a virus.
- **Repudiation:** A party to an online purchase denies that the transaction occurred or was authorized.
- **Forgery, Deception, Theft and Data Alteration:** These may result in theft or alteration of the content of a transaction -- user names, credit card numbers, and dollar amounts, for example- during transmission or in stored files.
- **Malicious Software:** This may also threaten the confidentiality and privacy of stored information.
- **Spoofing:** A fake site pretends to be the legitimate organization's and steals data from unsuspecting customers or just disrupt business.
- **Repudiation:** A party to an online purchase denies that the transaction occurred or was authorized.

Increased automation, sophistication of attack tools, faster discovery of vulnerabilities and increasing permeability of firewalls are among the key trends in computer attacks in the past few years, according to a recent report by CERT (Computer Emergency Response Team) Coordination Center, a federally funded research organization operated by Carnegie Mellon University. CERT-CC identified four types of infrastructure attacks, namely:

- 1) **Distributed Denial of Service:** This type of attack uses multiple systems to attack one or more victim systems. The main intent of the attack is to deny service to legitimate users of the victim systems.
- 2) **Worms:** A self-propagating malicious code that could attack a large number of systems globally in a matter of hours.

- 3) **Attacks on the Internet Domain Name System (DNS):** which include Cache-Poisoning, Compromised-Data, Denial of Service, and Domain-Hijacking.
- 4) **Attacks against/using Routers:** According to CERT-CC, intruders can use poorly secured routers as platforms to redirect traffic to other sites under their control.

According to the CERT-CC report, the level of automation and sophistication in attack tools continues to increase. "Today, scanning tools are using more advanced scanning patterns to maximize impact and speed," the CERT-CC report says. The report also notes that new attack tools allow attackers to devise attacks that can self-propagate at an incredible pace. "We have seen tools like Code Red and Nimda self-propagate to a point of global saturation in less than 18 hours." Attackers are also taking advantage of public communications protocols such as the Internet Relay Chat (IRC) and instant messaging to launch more coordinated attacks. Also, attackers' common use of the IRC or Internet protocol to send data or commands to victims' hosts makes it more difficult to differentiate it from normal network traffic.

It is interesting to note that according to CERT-CC, the number of newly discovered vulnerabilities more than doubles each year. This situation makes it more difficult for system administrators to keep up-to-date with software patches, hence, compromising the ability of their computer systems to counter attacks that exploit such vulnerabilities.

SECURITY PROBLEMS WITH SOLUTIONS

In this section we discuss some aspects of network security in the context of virtual marketing or e-commerce that have been partially or wholly solved with technology.

SECURE WEB CONNECTION

SSL (Secure Sockets Layer) is the security technology that is used most frequently to provide an encrypted link between a point in one computer system to a point in another computer system. SSL was developed by Netscape. It uses public key cryptography to secure messages from web browsers (clients) to Internet transaction servers (merchants). Information that flows between those two points is encrypted using a symmetric algorithm; 128 bit SSL uses a good algorithm to securely protect information traveling between two points in computer systems. SSL also uses digital certificates to verify the identity of the server. However, SSL does not offer a means to confirm the customer, merchant or financial institution involved in a given transaction.

SECURE PAYMENT

According to surveys conducted by CommerceNet, Inc. secure payments was listed in the "Top Ten Barriers for Retailing" and in the "Top Ten Consumer Barriers". According to Burns, an ideal secure payment system should have the following characteristics:

- **Ease of Automated Processing:** Automate the generation and processing of multiple payments with minimal effort.
- **Immediacy of Result:** The ability for the intermediate systems and providers to process payments in real-time.
- **Openness and Accessibility of Payment Processes:** Provide a range of payment services that were previously only available to large organizations via dedicated networks
- **Loss of Collateral Information:** The new technology dispenses with, or alters, collateral information (which is not essential) accompanying transactions
- **Globalization:** Minimization of geographical factors

Most e-businesses rely on established Internet transaction providers for their payment systems, which use debit and credit cards. The two most common security protocols used for this purpose are secure sockets layer (SSL) and secure electronic transaction (SET).

SET was developed by Visa International in conjunction with several other companies, and is widely used for debit and credit card transactions. SET uses digital certificates to identify the client (buyer), server (merchant), and merchant bank. SET employs public key cryptography to secure the messages between the three entities as they are transmitted over the Internet. SET allows the parties to confirm each other's identity. It uses digital certificates to allow a purchaser to confirm that the merchant is legitimate and allows the merchant to verify that the credit/debit card is being used by its owner. Lastly, it uses digital signature to identify the card holder to the retailer. These provide a certain level of trust, as well as protection from repudiation and unauthorized payments. It may be said of SET that it comes close to satisfying the five characteristics of a good payment system, as specified by Burns.

AUTHENTICATION – DIGITAL CERTIFICATES

As we saw, SET provides authentication by the use of digital signatures, which is the common means to provide authentication in e-commerce transactions. In general, customers and merchants generate these certificates through the mutual use of secret keys that shows the legitimacy of each party to the other. Most of these digital certificates conform to the X.509 standard, widely accepted as the best choice for digital certificates. X.509 compliant digital certificates are thought to strengthen simplicity and interoperability.

But, certificates do not completely solve the authentication problem, because the result is only as reliable as the process that created it.

IDENTITY

Identity is often mistaken for authentication. Establishing a physical identity requires a manual process. One of the most frequently used identity schemes is a token or a smart card, a small device carried by the remote user; based on a challenge-response system, the user is allowed or denied access to the remote system.

It is worth remembering that many e-commerce transactions do not require the knowledge of a physical identity, but some do. What is often needed is authorization, which is the granting of a privilege, and is also sometimes confused with authentication.

OTHER VULNERABILITIES

In October 2001 SANS and FBI, in combination with dozens of leading security experts from the government, industry and the two leading university-based security programs, CERT/CC and the SANS Institute, came up with a "Top twenty" list of vulnerabilities. The report also includes advice on how to correct this vulnerability. This list proved very valuable, especially to small and medium size organizations with Internet exposure and individuals. Subsequently, the Center for Internet Security has come up with an automated scanning tool to help check a system to see if it has each of the listed vulnerabilities. According to the Center for Internet Security, the majority of successful attacks against computer systems via the Internet can be traced to exploitation of un-patched vulnerabilities on this list.

INCREASED EMPHASIS ON QUALITY IN SOFTWARE AND SYSTEM DESIGN

The prevalent approach to network security has been one of "patchwork," a race against perpetrators and often one step behind. This is not the best way to operate and is enormously expensive and inefficient in the long term. Security has to be part of the design of the software. New standards of software quality need to take into account effective methods built into the software that would reduce or avoid the impact of current vulnerabilities. Newly developed information systems should be robust enough to withstand present and potentially new cyber attacks. It is a national challenge that needs to be addressed by the industry.

INTEROPERABILITY - LACK OF COORDINATED EFFORT IN SECURITY STANDARDS, TOOLS AND SOLUTIONS

There is a host of tools, solutions and standards addressing various aspects of network security promoted and supported by different standard bodies, vendors and groups. Some of the most popular security tools in use today, according to SANS are the following:

- **Host based Auditing Tools:** COPS, NCARP, Crack, Tiger, Tripwire, LogCheck, TKLogger, SafeSuite, NetSonar.
- **Network Traffic Analysis & Intrusion Detection Tools:** TCPDump, SynSniff, NetRanger, NOCOL, NFR, RealSecure, Shadow.
- **Security Management and Improvement Tools:** Crack, LocalMail, Smrsh, LogDaemon, NPasswd, OP, Passwd+, S4-kit, SFingerd, Sudo, Swatch, Watcher, Wuftpd, LPRng.
- **Firewall, Proxy and Filtering Tools:** FWTK, IPFilter, IPFirewall, PortMap V3, SOCKS, TCP_Wrappers, SMAPD.
- **Network based Auditing Tools:** NMap, Nessus, SATAN, SafeSuite.
- **Encryption Tools:** MD5, MD5Check, PGP, Rpm, UFC-Crypt.
- **One-Time Password Tools:** OPIE, S/Key.
- **Secure Remote Access and Authorization Tools:** RADIUS, TACACS+, SSL, SSH, Kerberos.

As this list would show, there are many diverging viewpoints, approaches, and methodologies that have given rise to a diverse set of solutions to some of the most pressing security problems. It is reasonable to assume that the best course of action would be for the government, industry and other security experts to work together to develop industry standard security solutions.

Interoperability is not limited to security issues alone. It is a pervasive problem, and undoubtedly the single most pressing issue that needs to be addressed if electronic commerce is to live up to its full potential. For electronic commerce to really succeed, interoperability must exist:-

- Between Technologies.
- Between Applications.
- Between Companies (especially between the e-commerce sites of complementary companies).
- Between Markets.
- Between Countries.

Furthermore, interoperability must exist with legacy systems. As Galvin points out interoperability is not just about technology and is one of the most critical barriers facing electronic commerce.

TRUST AND RISK

In all the surveys done by CommerceNet, there is not one issue that appears more often than trust and risk. "Trust is the grease in the wheels of commerce," says Professor Michael Rappa. Customers new to e-commerce worry about the integrity of seller organizations, merchants new to virtual marketing worry about the legitimacy of buyers and the validity of the payment of the goods and services, and so on and so forth. Yet, millions have come together in electronic market places such as eBay and successfully conduct business. eBay's Safe Harbor site is a very good example of enforcing trust.

Trusted third parties are often used to provide the "seal of approval." These include TRUSTe and WebTrust. Another approach, especially in large transactions, is the use of an escrow service. Yet another approach to solving this problem is the architecture for Public-Key Infrastructure (PKI) by the Open Group, one of whose required services is the "establishment of domains of trust and governance."

CONCLUSION

Digital enterprises can be managed more securely, and are being managed more securely than at any time in its short history. The magnitude of network security threats is large but it has not shunted the growth of virtual markets. With interoperability, a coordinated effort on the part of the key solution providers, and better overall security awareness in the design, implementation and operation of the computer systems, businesses ought to be able to more than keep pace with the criminals, terrorists, unethical businesses and customers.

REFERENCES

- 1) Center for Internet Security (2006). The "Top Twenty" automated scanning tool, <http://www.cisecurity.org/scanning_tool.html>
- 2) CERT Coordination Center (2010). Overview of Attack Trends, <http://www.cert.org/archive/pdf/attack_trends.pdf>
- 3) James A. Galvin (2005). EC Solutions – State of the Art. <<http://www.commerce.net>>
- 4) Michael Froomkin (2007). The Essential Role of Trusted Third Parties in Electronic Commerce, 75 Oregon L. Rev. 49, available at <http://www.law.miami.edu/~froomkin/articles/trusted.htm>
- 5) Stephen Burns (2008). Unique Characteristics of E-commerce Technologies and their effects upon Payment Systems, <http://rr.sans.org/ecommerce/payment.php>
- 6) The SANS Institute (2007). The Twenty Most Critical Internet Security Vulnerabilities, Updated Version 2.504, May 2, 2007, <http://www.sans.org/top20.htm>
- 7) The SANS Institute (2009). The Network Security Roadmap. <<http://www.sans.org/newlook/publications/roadmap.htm>>
- 8) Timothy J. Shimeall, Casey J. Dunlevy, Phil Williams. (2011) Intelligence Analysis for Internet Security: Ideas, Barriers and Possibilities. CERT Analysis Center, Software Engineering Institute, Carnegie-Mellon University, available from: <http://www.cert.org/archive/html/spie.html>

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Commerce, IT 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-mail i.e. **infoijrcm@gmail.com** 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

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals

