



A STUDY ON CYBER FRAUDS IN INDIAN BANKING SECTOR

A. V. B. N. H. Saroja* & Dr. Raavi Radhika**

* Research Scholar, Hyderabad Business School, GITAM University,
Hyderabad, Telangana

** Associate Professor, Hyderabad Business School, GITAM University,
Hyderabad, Telangana

Cite This Article: A. V. B. N. H. Saroja & Dr. Raavi Radhika, "A Study on Cyber Frauds in Indian Banking Sector", International Journal of Applied and Advanced Scientific Research, Volume 3, Issue 1, Page Number 315-321, 2018.

Abstract:

The number of cyber frauds increasing substantially during the advent of Information Technology. Due to liberalization, privatization and globalization it became necessary for the banks to go with online banking. In the modern era, increase in the number of smart phone users leads to increase in mobile banking and mobile wallets transactions. Frauds related to online banking transactions viz., RTGS (Real-Time Gross Settlement Systems), ECS (Electronic Clearing Service), usage of mobile banking transactions and mobile wallets are known as "Cyber Frauds". Over a period, the nature and pattern of Cyber Crime have become more complex and sophisticated. The study focused on the present scenario of Cyber frauds in Indian Banking sector. Based on the primary data collected from nationalized, private sector and foreign banks in India the present scenario of cyber frauds is being analysed. The survey by Ernest & Young, 2012 reports that 84% of the fraud cases recorded from the financial services sector. The customers expect transparency, privacy standards, accountability and security from effective intermediation from banks. The channels for cyber-crimes are through computer, computer network or communication devices, mobile phones and mobile networks etc., with the enhancement of the cyber security standards cyber-attacks and crimes can be prevented in future for enhanced society. The present paper focuses on the technical aspects of various types of cybercrimes concerning the Indian Banking sector.

Key words: Cyber Fraud, Information Technology, Privacy, Security & Transparency

Introduction:

Introduction of technology made our life easy; however, there is risk of cyber frauds by misuse of technology. The world has been witnessing a raising trend of using online transactions, digital data transfer, electronic database and so many business, social and other activities based on computers, internet and information technology tools. Many innocent individuals fall victim to cybercrimes around the world. When the confidential information is lost or interrupted unlawfully, it leads to high profile crimes such as cyber terrorism, financial theft, copyright infringement, hacking etc., Cybercrimes are growing every day because of technological advancement in computers made easy to steal the data from computers. Understanding the threat of cybercrimes is very important and has impact on our society as a whole. Advancement in technology and fast internet made customers to depend on digital payment services. The services like checking bank balance, request for bank statements and cheque books, up gradation of debit cards even purchasing virtual goods. Now-a-days financial institutions are using social media platforms to engage their customers for online payments. Recently one of the largest private sector banks in India launched a multi-social payment app that allows customers to make money transfer through social media channels. 65% of the fraud cases reported by banks were related to technology frauds i.e. frauds committed through or at an internet banking channel, ATMs and other payments channels like debit/credit/prepaid cards. Cyber frauds are extremely technological crimes. Solving cyber frauds is a challenging task for law enforcement bureaus. Law enforcement bureaus must have technically sound staff in computer forensics to investigate cybercrimes.

"RBI has mandated that all unusual cyber-incidents have to be reported within 2 to 6 hours invariably. We observe that banks take much longer time in reporting the incident", by Mundra in a seminar on Financial Crimes Management recently.

Objectives of the Study:

- ✓ To study the concept of Cyber frauds in Public and Private sector banks.
- ✓ To make meaningful analysis of the data belonging to banking cyber frauds of different banking sectors.

Methodology:

Secondary data published by Reserve Bank of India has been taken to the present study. Tables and graphs have been used for comparative analysis. Though the present study is related to comparative analysis between private and public-sector banks, data related to foreign banks also taken for study to know their share in cybercrimes, since they belong to private sector only.

Review of Literature

Beirstaker, Brody, Pacini (2005) has suggested various techniques like fraud vulnerability reviews, telephone hotlines, fraud policies, employee reference checks, vendor contract reviews (financial ratio analysis

etc.), password protection, firewalls protection, digital analysis and other forms of software tools to detect and control frauds.

Gupta P. K. (2008) in his study 'Internet Banking in India- Consumer Concerns and Bank Strategies' tried to explore the weaknesses of conventional banking and the consumer awareness, user patterns, preferences and satisfaction or Intent banking and also highlighted the factors that affect the bank's strategy to adopt Internet banking. His study also addressed the regulatory and supervisory concerns of Internet banking.

Ashu Khanna, Bindu Arora (2009) in their survey based work 'A study to investigate the reasons for bank frauds and implementation of preventive security controls in Indian banking industry' and to find out the attitude and measures taken by bank employees/managers in controlling banking cybercrimes. It is observed that bank employees do not give due importance to the problem of frauds. The awareness level of bank employees regarding bank frauds is not very satisfactory, and majority of them do not dispose favourable attitude towards RBI procedures as they find difficulty in following them due to workload and pressure of competition.

Hemraj Saini, Yerra Shankar Rao & T. C. Panda (2012) in their study 'Cyber-Crimes and their Impacts: A Review' has described the problem and kinds of cybercrimes with their effects on different segments in the society in general.

B. Singh (2013) in their report 'Online Banking Frauds in India' has observed that Cybercrimes in India are on rise. With limited numbers of cyber law firms in India, these cybercrimes are not reported properly. Even the cyber security of India is still catching up with the present requirements.

Definition of Fraud:

The word Fraud defined as "any behaviour by which one person intends to gain a dishonest advantage over another". The wrongful gain or loss which one person gets out of an act or omission to the other, either by way of concealment of facts or otherwise. Fraud is defined under section 421 of the Indian Penal Code and under section 17 of the Indian Contract Act.

The underlying dimensions is defined how the involvement of technology in the electronic crime. Using the Graham's (2001) definition the following diagram represents the e-fraud as the intersection of E-crime and Fraud.

Types of Cyber Frauds:

Hacking: Fraudsters/hackers obtain unauthorised access to the card management platform of banking system.

Triangulation/Site Cloning: The customers unknowingly enter their card details on the fraudulent shopping sites.

- ✓ **Online Fraud:** Fraudsters will steal the card details at the time of an online transaction.
- ✓ **Electronic Fraud:** This refers to email scams from fraudsters to obtain banking and personal information. The person receives an email from a company claiming some information about the customer's bank account details. Those are:
 - saying that problem with your account
 - ask you to enter a contest to win a prize
 - ask you to subscribe to a service to win prize etc.,When you provide your personal and financial information - by completing an online form – which includes your credit card numbers – your account number – your passport or Civil ID number and so forth.
- **Wire fraud:** international or interbank fund transfer system is a transfer system, once made, is impossible to reverse. Huge amounts or overnight wire transfer of amounts of money is common place, there is risk that insiders may try to attempt fraudulent or forged documents to request a bank depositor's money to be wired to another bank, often an offshore distant foreign country account.

Debit Card Skimming: fraudsters install a machine or camera at an ATM to pick up card information and PIN numbers when customers doing the transactions using their cards. Debit and credit cards are reproduced by criminals; this is called 'skimming'. Credit or debit card fraud also occurs when the fraudster uses the stolen card to purchase goods or remove cash from ATMs or at other locations. Credit card fraud leads to a huge loss for banks and the government

Lost/Stolen Card: fraudsters will use the stolen card unauthorised/illegal purposes.

Computer Viruses: with every click on internet, a company's systems are open to the risk of being infected with malware.

Dumpster Diving: Due to negligence of employees who throw away papers containing sensitive information, can be stolen by the fraudsters.

Identity Fraud: Identity fraud is where a fraudster will gather personal details to do frauds which will financial hurt to the user. The personal information can obtain by user in different ways via telephone scams or on the internet. Date of Birth - address - personal ID number or other identification numbers - Mobile phone number - Banking information.

Booster Cheques: It is a method used to make payment to a credit card account through a bad or fraudulent cheque to 'bust out' or increase the availability of credit. The banker will credit the amount as soon as the payment is received from customer irrespective of clearance of cheque. The card holder will utilise the available credit before the original cheque bounces.

The dishonest merchant copying client's credit card numbers and later misuses the card details. The contents of the magnetic stripe will be captured through a fraudulent card stripe. A hidden camera will tamper credit or debit card details and pick of user's PIN. The fraudulent equipment uses the data to produce duplicate cards and then use for ATM withdrawals from the victims' accounts.

Cyber Frauds in India:

- ✓ Nearly 12,000 cases related to credit/debit cards and net banking were reported during April-December 2015.
- ✓ During 2014-15 and 2015-16 (up to December 2015) 13,083 and 11,997 ATM/ Credit / Debit card cases reported.
- ✓ As per records maintained by National Crime Records Bureau (NCRB) , a total of 5,693 and 9,622 cybercrime cases reported under IT Act,2000 and Indian Penal Code (IPC) and Special Local Laws (SLL) during 2013 and 2014 respectively.
- ✓ In 2009, the internet fraud has resulted in a loss of 6.6 Crores in 233 reported cases.
- ✓ Between April to December 2009 over 13,000 credit card fraud cases were reported as per Orissa government statistics.
- ✓ In 2008, the credit card frauds in 2994 cases involving ₹532 lakhs
- ✓ In 2005 – 2658 cases; 2006 – 2568 and in 2007 – 2933 in public sector banks as per RBI report.
- ✓ In ICICI Bank reported a loss of 1147 lakh out of 8280 cases.

Discussion and Analysis:

Reserve Bank of India (RBI) is the regulatory body over banking in India. RBI closely monitors the banking operations. RBI published the details of cyber frauds relating to ATM/Debit Cards/Credit Cards/ Internet Banking in Scheduled Commercial Banks. Table-1 shows the details as under:

Table-1

Cyber Frauds in Scheduled Commercial Banks from 2009-12

S.No.	Calendar Year	Total cases reported	Amount involved
1	2009	21966	7233.31
2	2010	15018	4048.94
3	2011	9588	3672.19
4	2012	8322	5266.95

(Source: <http://www.rbi.org.in/>)

Cyber Frauds in Scheduled Commercial Banks from 2009-12

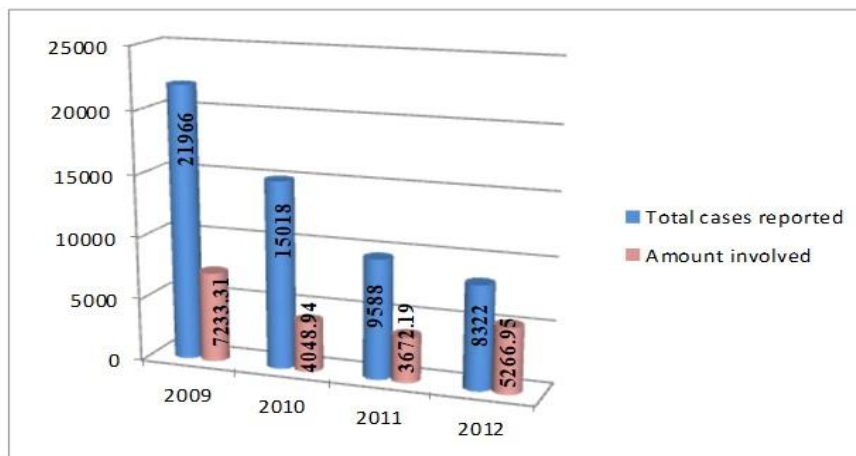


Figure.3

Interpretation: the above table-1 and Figure-1 show reducing number of reported cases. The amount involved is also reducing but in 2012 shows an increase. The number of cases fell by 31.6%, 36.2%, and 13.2% in the year 2010, 2011, and 2012 respectively. The amount involved also came down by 44.0%, 9.3% in 2010 and 2011 respectively, but in 2012 it rose by 43%.

Comparative Analysis: The data have been analysed to reveal comparative status of fraud cases in terms of numbers and amounts involved. The study highlights two comparisons (i) intra sector comparison (ii) inter banking comparisons.

Table - 2
Details of Cyber Frauds in Public Sector Banks - Year Wise

S.No.	Bank name	2009		2010		2011		2012	
		No.of Cases	Amount involved	No.of Cases	Amount involved	No.of Cases	Amount involved	No.of Cases	Amount involved
1	Allahabad Bank	0	0	0	0	1	3.3	0	0
2	Andhara Bank	0	0	1	31.85	1	0.52	0	0
3	Bank of Baroda	6	6.88	5	12.4	5	31.82	3	62.45
4	Bank of India	5	5.21	2	14.61	2	54.49	7	15.82
5	Bank of Maharashtra	4	3.55	4	4.69	2	2.9	3	105.26
6	Bank of Rajasthan Ltd	0	0	1	0.31	0	0	0	0
7	Canara bank	6	1.39	0	0	1	0.6	1	10.24
8	Central bank of India	2	0.84	2	2.15	0	0	0	0
9	Corporation Bank	2	0.72	2	6.21	5	6.44	47	21.69
10	Dena Bank	0	0	1	2.07	1	0.53	0	0
11	FirstRand Bank	0	0	0	0	0	0	14	4.82
12	IDBI Bank Limited	24	16.29	13	15.29	50	44.64	87	203.04
13	Indian Bank	0	0	1	1.41	1	0.41	4	20.9
14	Indian Overseas Bank	2	0.39	3	1.44	10	176.03	0	0
15	Oriental Bank of Commerce	0	0	1	4.75	0	0	0	0
16	Punjab National bank	33	50.15	108	248.64	28	170.19	14	99.43
17	SBBJ	2	6.66	2	0.15	2	3.49	1	49.32
18	State Bank of Hyderabad	0	0	0	0	4	63.33	6	50.52
19	State Bank of India	0	0	0	0	2	14.62	0	0
20	State Bank of Indore	1	0.8	0	0	0	0	0	0
21	State Bank of Mysore	0	0	1	1.01	0	0	0	0
22	State Bank of Patiala	0	0	0	0	4	80.45	2	31.42
23	State Bank of Travencore	0	0	0	0	6	10.3	3	3.2
24	Syndicate Bank	2	0.53	1	2.32	1	0.56	2	7.87
25	UCO Bank	2	0.58	1	1.6	0	0	4	31.22
26	Union Bank of India	5	10.45	7	19.22	2	7.86	9	70.17
27	United Bank of India	1	1.37	0	0	0	0	6	32.86
28	Vijaya Bank	0	0	0	0	0	0	1	8.4
Grand Total		97	105.81	156	370.12	128	672.48	214	828.63

(Source: Details of Calendar Year Wise Cyber Frauds in Banks www.rbi.org.in)

Interpretation: In table 2 it is observed that number of cyber fraud cases in public sector banks increasing during the given four year's period. The amount involved had in rising tendency. In year 2010, the highest number of cyber frauds cases recorded in PNB and followed by IDBI bank. Again, in year 2010, the highest number of cyber frauds recorded in PNB and followed by IDBI bank but amount wise Andhra Bank, Union Bank of India and IDBI respectively. IDBI crossed PNB in 2011 in terms of number of cases, but Indian Overseas, PNB and Bank of Patiala witnessed a substantial rise. In 2012, IDBI came on top Corporation bank and PNB. In terms of money involved IDBI, Bank of Maharashtra and PNB recorded highest positions respectively.

Details of Calendar Year Wise Cyber Frauds in Public Sector Banks

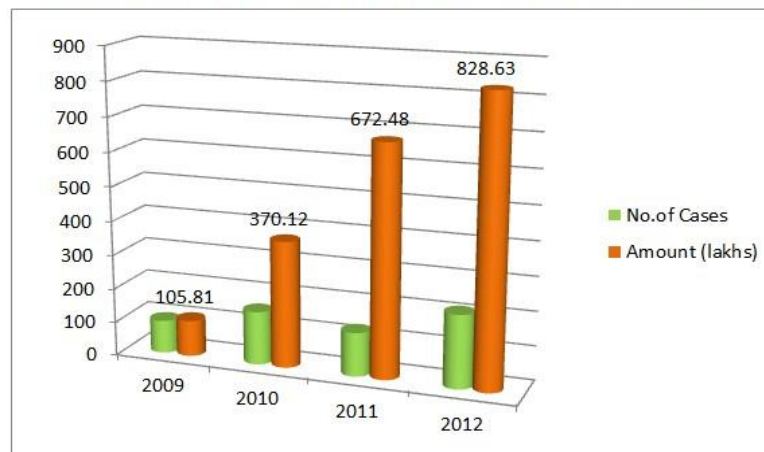


Figure.4

Table-3

Details of Cyber Frauds in Private Sector Banks - Year Wise									
(Amount in lakhs)									
S.No.	Bank name	2009		2010		2011		2012	
		No.of Cases	Amount involved	No.of Cases	Amount involved	No.of Cases	Amount involved	No.of Cases	Amount involved
1	Axis Bank Ltd	20	110.58	14	44.59	23	209.59	85	1225.41
2	Development Credit Bank	2	0.96	2	0.3	0	0	0	0
3	Dharalakshmi Bank Ltd	0	0	3	2.29	1	3.02	4	1.09
4	Federal Bank Ltd	0	0	2	20.5	0	0	3	83.69
5	HDFC Bank Ltd	211	165.58	208	125.98	386	276.68	525	409.56
6	ICICI Bank Ltd	15666	3731.95	9811	1920.28	6013	1096.67	3428	676.51
7	IndusInd Bank Ltd	0	0	3	7.59	3	1.19	2	4.61
8	Jammu & Kashmir Bank	1	4.51	2	6.58	0	0	1	13.88
9	Karur Vysya Bank Ltd	0	0	1	23.14	0	0	0	0
10	Kotak Mahindra Bank Ltd	57	75.26	31	29.63	52	33.11	78	67.64
11	Lakshmi Vilas bank Ltd	0	0	0	0	0	0	1	10
12	South Indian Bank Ltd	1	2.47	1	0.54	2	0.84	2	0.49
13	Tamilnad Mercantile Bank	0	0	0	0	1	0.27	1	1.49
14	The Royal Bank of Scott.	142	141.3	51	44.52	46	49.35	14	12.1
Grand Total		16100	4232.61	10129	2225.94	6527	1670.72	4144	2506.47

(Source: Details of Calendar Year Wise Cyber Frauds in Banks www.rbi.org.in)

Interpretation: In Table-3 it is observed that number of cyber fraud cases in private sector banks had largest share in banking sector not only in number of cases but also in terms of money. The number of cases recorded in 2009 is 16100 and it came down to 4144 in 2012. Similarly, the amount also came down from 4232.61 lakhs in 2009 to 1670.72. But again, it rose to 2506.47 in 2012. However overall declined trend has observed in cyber frauds in private sector bank. ICICI bank had highest position in cyber frauds during the four years period in number of cases and high volumes also. HDFC and Axis Banks followed the position respectively with a sudden rise in value by Axis Bank in 2012.

Table-4

Details of Cyber Frauds in Foreign Banks - Year Wise									
(Amount in lakhs)									
S.No.	Bank name	2009		2010		2011		2012	
		No.of Cases	Amount involved	No.of Cases	Amount involved	No.of Cases	Amount involved	No.of Cases	Amount involved
1	American Express Banking Corp.	980	904.57	819	360.75	908	522.76	1231	816.99
2	Barclays Bank Plc	35	21.68	48	8.38	14	6.03	7	1.11
3	Citi bank N.A.	1226	773.18	925	521.27	774	420.01	1504	690.32
4	Deutsche Bank (Asia)	61	116.64	35	81.94	9	13.67	2	34.74
5	Hong Kong & Shanghai banking Corporation Ltd	3093	722.45	2520	293.02	793	181.41	709	180.73
6	Standard Chartered Bank	374	356.37	386	187.52	435	185.11	511	207.96
Grand Total		5769	2894.89	4733	1452.88	2933	1328.99	3964	1931.85

(Source: Details of Calendar Year Wise Cyber Frauds in Banks www.rbi.org.in)

Interpretation: In table-4 it is observed that number of cyber fraud cases recorded in foreign banks at a greater extent. HSBC had largest share in 2009, has corrected the situation up to 2012. Other two leading banks Citibank and American Express have suppressed HSBC.

Interpretation: In figure-3 shows the number of cyber fraud cases from 2009-2012. It is observed that private sector banks have gone far away recording very large number of cases. Foreign banks also have monetary loss and have bad picture. A substantial drop has been noticed in both private and foreign banks. Public sector banks show a nominal number of cases.

Bank Sector-wise No. of Cases

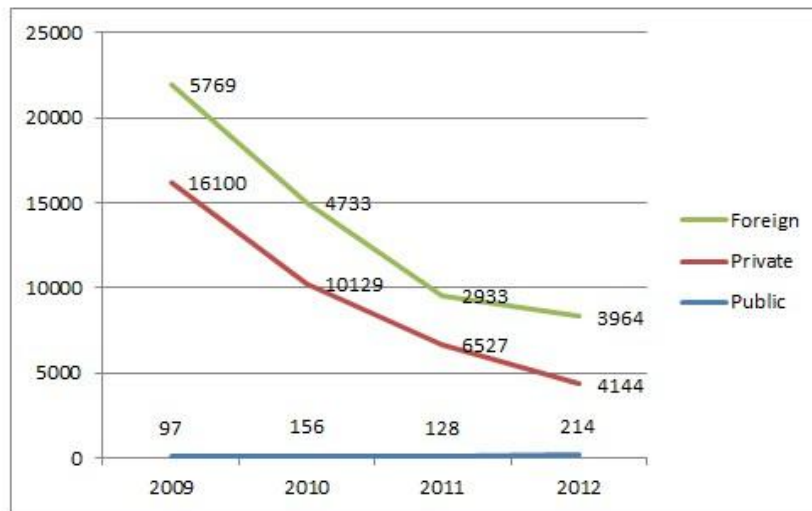


Figure.5

Bank Sector-wise Amount involved (in lakhs)



Figure.6

Interpretation: Monetary involvement in fraud cases has been shown in figure-4. Both private sector banks and foreign banks a head of public sector banks. After a declining trend up to 2011, the value again ascended in 2012.

Recent Cyber incidents:

- ✓ Bitfinex, August 2, 2016, A Hong Kong exchange for the trading of digital currencies, announced that some of its customer accounts were hacked and bitcoins stolen. The approximate value of stolen bitcoins has been reported as US\$65 million or more. As a consequence of this incident, the value of bitcoins came down and the trust on digital currency shaken.
- ✓ The Bangladesh Bank was targeted and attempt to steal US\$1 billion and finally the attackers could successfully get away with US\$81 million.

- ✓ Recently in India also, a similar attempt was made on a commercial bank by giving fraudulent payment instructions on the Nostro accounts and transmitting them over SWIFT messaging system. Finally, monetary loss could be prevented with proactive follow-up, but this incident proved the fact that the various stakeholders have not learnt the lessons yet.
- ✓ In another incident, e-payment validation website of a large bank was hacked. The bank was not aware of the incident till it was notified by a law enforcement agency. It was posted by a person from neighbouring country claiming responsibility for the operation in the Face book.

Regulatory and Legislative Landscape:

A master circular issued by RBI on 'Frauds – Classification and Reporting'. The circular fixed the significance of preventing frauds in Banks and make them into a completely new horizon of financial risks. RBI instructed banks to report the "complete information about frauds and the follow up action taken thereon". Now with robust reporting and risk monitoring system, banks can control financial and reputational risks more efficiently. RBI has issued guidelines to regulate and suggested to report of doubtful transactions to its financial intelligence unit. The Banks, by using advanced tools and technology keep a check on frauds should deploy greater level of scrutiny against unethical activities.

The information Technology Act, 2000, was passed as the Act No.21 of 2000, got President assent on 9th June and was made effective from 17th October 2000. Being the first legislation in the nation, the IT Act, 2000 faced many criticisms. Though IT act 2000 was the first step towards combating cybercrimes and encouraged e-commerce in India, the act was not implemented properly. IT Act 2000 was again revised in 2010 with more stringent laws to counter ever increasing cyber frauds in India.

Conclusion:

Title of the study showed a large share of cyber frauds in private and foreign banks. The cyber frauds mainly involved in online banking, ATM cards and other digital related fraud banking transactions. The regulator frame work is also strengthened by the experience. The RBI has issued different methods of cyber fraud reporting guidelines to be followed by bank.

References:

1. BS_ViewBulletin. (n.d.). Retrieved from https://www.rbi.org.in/scripts/BS_ViewBulletin.aspx?Id=14351 , viewed on 28th Dec,2017
2. Charan Singh & Others. (2016, March). Frauds in the Indian Banking Industry. Retrieved from IIMB-WP No.505: <https://www.iimb.ac.in/research/sites/default/files/WP%20No.%20505.pdf>
3. current-fraud-trends-in-the-financial-sector. (n.d.). Retrieved from [www.pwc.in](https://www.pwc.in/assets/pdfs/publications/2015/current-fraud-trends-in-the-financial-sector.pdf): <https://www.pwc.in/assets/pdfs/publications/2015/current-fraud-trends-in-the-financial-sector.pdf> viewed on 11th December, 2017
4. Cyber e-Bulletin 20jan-2017. (n.d.). Retrieved from [http://mahacid.com/](http://mahacid.com/Cyber%20e-Bulletin%20jan-2017.pdf): <http://mahacid.com/Cyber%20e-Bulletin%20jan-2017.pdf>, viewed on 28th Dec,2017
5. Dangolani, S. K. (2011). "The Impact of Information Technology in Banking System (A Case Study in Bank Keshavarzi IRAN). *Procedia Social and Behavioral Sciences*, *www.sciencedirect.com*.
6. Dr.Ashvine Kumar & Ms.Priyanka. (October 2013). An Investigation of Banking Cyber Frauds with Indian Private and Public Sector Banks. *International Journal of 360 degrees Management Review* , Vol1, Issue2.
7. *economictimes*. (n.d.). Retrieved from <https://economictimes.indiatimes.com/industry/banking/finance/banking/public-sector-banks-at-a-higher-threat-of-cyber-attack-than-private-banks-says-rbi-dg/articleshow/56948000.cms> viewed on 28th Dec,2017
8. Financial-Foresights-April-2017. (n.d.). Retrieved from [http://ficci.in/](http://ficci.in/sector/3/Add_docs/Financial-Foresights-April-2017.pdf): http://ficci.in/sector/3/Add_docs/Financial-Foresights-April-2017.pdf , viewed on 28th Dec,2017
9. Gupta P.K. (2008). Internet Banking in India – Consumer concerns and Bank strategies. *Global Journal of Business Research*, 2(1).
10. Impact-of-Cyber-Attacks-on-the-Private-Sector. (n.d.). Retrieved from <https://www.mindpointgroup.com/wp-content/uploads/2014/08/Impact-of-Cyber-Attacks-on-the-Private-Sector.pdf> , viewed on 28th Dec,2017
11. Khanna Ashu & Arora Bindu. (2009). A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian Banking industry. *Int. J. Bus. Sci. & App. Mgmt.* 4(3). (2009).
12. PublicationReportDetails. (n.d.). Retrieved from <https://www.rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage=&ID=722>, viewed on 29th Dec,2017
13. shodhganga. (n.d.). Retrieved from [http://shodhganga.inflibnet.ac.in/](http://shodhganga.inflibnet.ac.in/bitstream/10603/74801/9/chapter%203.pdf), viewed on 11th Dec, 2017: <http://shodhganga.inflibnet.ac.in/bitstream/10603/74801/9/chapter%203.pdf>
14. Soni R.R & Soni Neena. (n.d.). "An Investigation study of Banking Cyber Frauds with special reference to Private and Public Sector Banks". *Research Journal of Management Sciences* Vol.2(7),22-27, July (2013), <http://www.isca.in/IJMS/Archive/v2/i7/4.ISCA-RJMS>