ARUNAI PUBLICATIONS

Asian Journal of Multi-Disciplinary Research

DOI: http://dx.doi.org/10.20468/ajmdr.2018.02.13

Research Article

A Study on Cyber Frauds in Indian Banking Sector

A. V. B. N. H. Saroja, Raavi Radhika

Hyderabad Business School, Gandhi Institute of Technology and Management University, Hyderabad, Telangana, India

Address for correspondence:
A. V. B. N. H. Saroja, Hyderabad Business School, Gandhi Institute of Technology and Management University, Hyderabad, Telangana, India

ABSTRACT

The number of cyber frauds increases 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, namely, real-time gross settlement systems, electronic clearing service, usage of mobile banking transactions, and mobile wallets are known as "cyber frauds." Over a period, the nature and pattern of cybercrime 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 analyzed. The survey by Ernest and Young, 2012, reports that 84% of the fraud cases recorded from the financial services sector. The services such as checking bank balance, request for bank statements and cheque books, upgradation of debit cards even purchasing virtual goods. The customers expect transparency, privacy standards, accountability, and security from effective intermediation from banks. Cyber frauds are technological crimes. The channels for cybercrimes are through computer, computer network or communication devices, mobile phones, and mobile networks; with the enhancement of the cybersecurity 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.

Keywords:
Cyber fraud,
Information technology,
Privacy,
Security,
Transparency

Received: 25th January 2018
Accepted: 20th February 2018
Published: 30th May 2018

INTRODUCTION

Introduction of technology made our life easy; however, there is a 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, and hacking. 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. Nowadays, 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 multisocial 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 such as 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.

"Reserve Bank of India (RBI) has mandated that all unusual cyber-incidents have to be reported within 2–6 h invariably. We observe that banks take much longer time in reporting the incident," by Mundra in a seminar on Financial Crimes Management recently.[1]

Objectives of the study

The objectives of this study are as follows:

- 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 RBI have been taken to the present study. Tables and graphs have been used for comparative analysis. Although the present study is related to comparative analysis between private and public sector banks, data related to foreign banks were also taken for study to know their share in cybercrimes, since they belong to private sector only.

REVIEW OF LITERATURE

Pacini (2005) has suggested various techniques such as 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 (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 internet 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.

Khanna and 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 favorable attitude toward RBI procedures as they find difficulty in following them due to workload and pressure of competition.

Hemraj *et al*. (2012) in their study "cyber-crimes and their Impacts: A review" have described the problem and kinds of cybercrimes with their effects on different segments in the society in general.

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 behavior by which one person intends to gain a dishonest advantage over another."[2] The wrongful gain or loss which one person gets out of an at 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 (IPC) and under section 17 of the Indian Contract Act.[3]

The underlying dimensions are defined how the involvement of technology in the electronic crime.

TYPES OF CYBER FRAUDS[4]

Hacking

Fraudsters/hackers obtain unauthorized access to the card management platform of banking system.

Triangulation/site cloning

The customers unknowingly enter their card details on the fraudulent shopping sites.

a. **Online fraud:** Fraudsters will steal the card details at the time of an online transaction.
b. **Electronic fraud:** This refers to e-mail 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 as follows:

- 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, and once made, is impossible to reverse. Huge amounts or overnight wire transfer of amounts of money is common place, and there is a 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 do 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 unauthorized/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 through telephone scams or on the internet such as date of birth, address, personal ID number or other identification numbers, mobile phone number, and 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 utilize the available credit before the original cheque bounces.
- The dishonest merchant copies 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 uses 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 2014–2015 and 2015–2016 (up to December 2015), 13,083 and 11,997 ATM/Credit/Debit card cases reported.
- As per records maintained by the National Crime Records Bureau, a total of 5,693 and 9,622 cybercrime cases reported under IT Act, 2000, and IPC and special local laws 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 and 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 involve 532 lakhs.
- In 2005,2658 cases; in 2006, 2568; and in 2007,–2933 in public sector banks as per RBI report.
- ICICI Bank reported a loss of 1147 lakh out of 8280 cases.

DISCUSSION AND ANALYSIS

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.[5] Table 1 shows the details about cyber frauds in scheduled commercial banks from 2009 to 2012.

Interpretation

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% and 9.3% in 2010 and 2011, respectively, but in 2012, it rose by 43%.

COMPARATIVE ANALYSIS

The data have been analyzed to reveal comparative status of fraud cases in terms of numbers and amounts involved. The study highlights two comparisons: (i) Intrasector comparison and (ii) interbanking comparisons.

Interpretation

In Table 2, it is observed that a number of cyber fraud cases in public sector banks increase during the given 4 year's period. The amount involved had in rising tendency. In the 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.

Interpretation

In Table 3, it is observed that a 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. However, 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 4 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.

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 and has corrected the situation up to 2012. Other two leading banks, Citibank and American Express, have suppressed HSBC.

Interpretation

Figure 3 shows the number of cyber fraud cases from 2009 to 2012. It is observed that private sector banks have gone far

Table 1: Cyber frauds in scheduled Commercial Banks from 2009 to 2012

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/

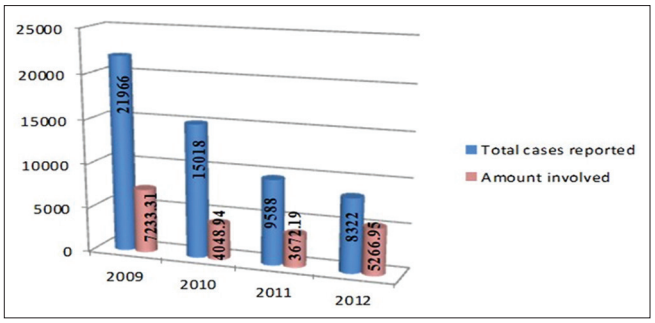

Figure 3: Cyber frauds in scheduled Commercial Banks from 2009 to 2012

Table 2: Details of cyber frauds in public sector banks - year wise

S. No	Bank name	(Amount in lakhs)							
		2009		2010		2011		2012	
		Number of cases	Amount involved	Number cases	Amount involved	Number of cases	Amount involved	Number of cases	Amount involved
1	Allahabad Bank	0	0	0	0	1	3.3	0	0
2	Andhra 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.ois.in

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.

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 bit coins stolen. The approximate value of stolen bit coins has been reported as US$65 million or more. As a consequence of this incident, the value of bit coins 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.

Table 3: Details of cyber frauds in private sector banks - year wise

S. No	Bank name	(Amount in lakhs)							
		2009		2010		2011		2012	
		Number of cases	Amount involved	Number of cases	Amount involved	Number of cases	Amount involved	Number 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	Dhanalakshmi 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	119	2	4.61
8	Jammu and 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)

Table 4: Details of Cyber Frauds in Foreign Banks - year wise

S. No	Bank name	(Amount in lakhs)							
		2009		2010		2011		2012	
		Number of cases	Amount involved	Number of cases	Amount involved	Number of cases	Amount involved	Number 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	Citibank 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 and 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 mw.rbi.org.in

- 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 neighboring country claiming responsibility for the operation in the Facebook.

REGULATORY AND LEGISLATIVE LANDSCAPE

A master circular was issued by RBI on "Frauds - Classification and Reporting."[6] 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."[6] 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, using advanced tools and technology, keep a check on frauds should deploy greater level of scrutiny against unethical activities.

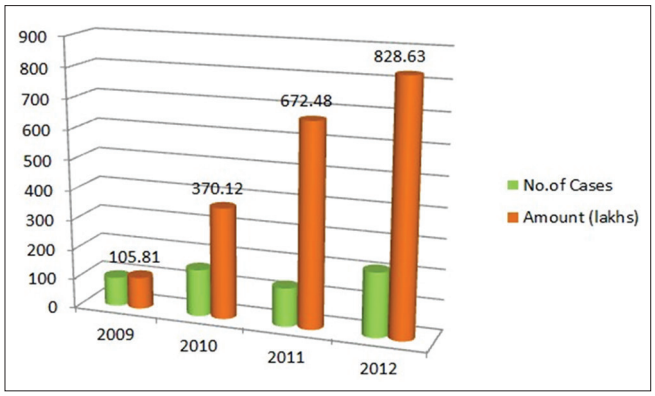

Figure 4: Details of calendar year wise cyber frauds in public sector banks

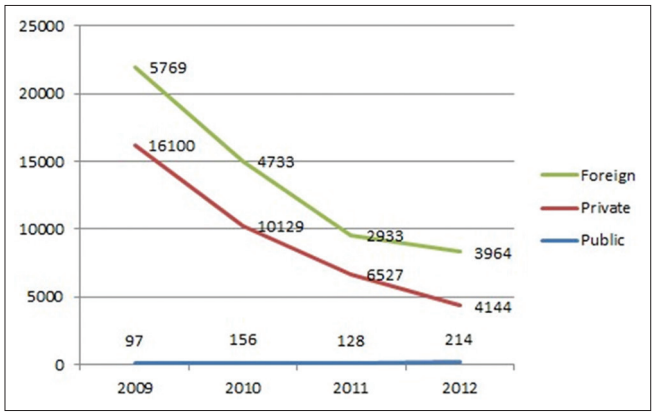

Figure 5: Bank sector-wise number of cases

The Information Technology Act, 2000, was passed as the Act No. 21 of 2000, got President Assent on June 9 and was made effective from October 17, 2000. Being the first legislation in the nation, the IT Act, 2000, faced many criticisms. Although the IT act 2000 was the first step toward combating cybercrimes and encouraged e-commerce in India, the act was not implemented property. The IT Act 2000 was again revised in 2010 with more stringent laws to counter ever increasing cyber frauds in India.[7]

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.

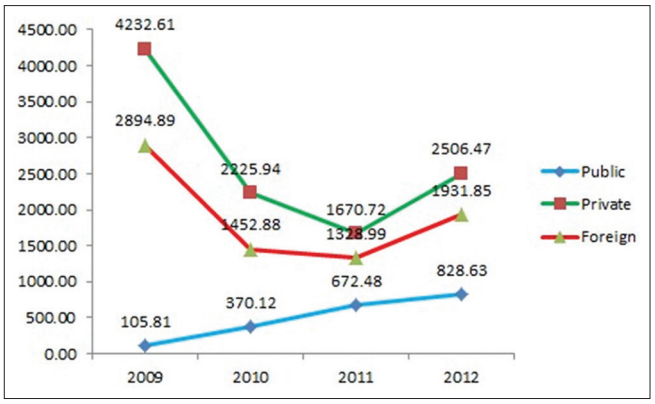

Figure 6: Bank sector-wise amount involves (in lakhs)

REFERENCES

1. Mundra SS. Fraud Risk Management in Banks: The Do's and Don'ts; 2017. Available from: https://www.rbidocs.rbi.org.in/rdocs/Bulletin/PDFs/2FRAUD9C31889A6C9C46E7858BED474DAA6E5F.PDF. [Last viewed on 2017 Dec 26].
2. Nainta RP, Sharma BR. Banking System, Frauds and Legal Control; 2005. Available from: https://www.books.google.co.in/books?id. [Last viewed on 2017 Dec 26].
3. BS_ViewBulletin. (n.d.). Available from: https://www.rbi.org.in/: https://www.rbi.org.in/scripts/BS_ViewBulletin.aspx?Id=14351 [Last viewed on 2017 Dec 28].
4. Assocham India, Current-Fraud-Trends-in-the-Financial-Sector. (n.d.).; 2015. Available from: https://www.pwc.in/assets/pdfs/publications/2015/current-fraud-trends-in-the-financial-sector.pdf. [Last viewed on 2017 Dec 11].
5. Kumar A, Priyanka. An investigation of banking cyber frauds with indian private and public sector banks. Int J 360 Degrees Manage Rev 2013;1.
6. Assocham India, Current-Fraud-Trends-In-The-Financial-Sector. (n.d.); 2015. Available from: https://www.pwc.in/assets/pdfs/publications/2015/current-fraud-trends-in-the-financial-sector.pdf. [Last viewed on 2017 Dec 11].
7. Shodhganga. (n.d.). Available from: http://www.shodhganga.inflibnet.ac.in; http://www.shodhganga.inflibnet.ac.in/bitstream/10603/74801/9/chapter%203.pdf. [Last viewed on 2017 Dec 11].

Cite this article: Saroja AVBNH, Radhika R. A Study on Cyber Frauds in Indian Banking Sector. Asian J Mult-Disciplinary Res. 2018;4(2):57-62.

Source of Support: Nil, **Conflict of Interest:** None declared.