International Journal of Education and Science Research
REVIEW E-ISSN 2348-6457
Volume-3, Issue-3 June- 2016
www.ijesrr.org Email- editor@ijesrr.org

CYBER CRIME IN INDIAN BANKING SECTOR

Dr. Ashvine Kumar Sharma
Research Guide
Associate Professor
Hindu Institute of Management
Sonipat

Ms. Priyanka
Research Scholar
Mewar University Chittorgarh
Rajasthan

ABSTRACT: In the present globalizes scenario, information technology is the most significant and disputable Time period. It is the most powerful era which is fast, quick and accurate in all sectors. Increased uses of information and communication technology (ICT) like as computers, mobile phones, Internet, and alternative associated technologies are the routes which gave emergence to lot of constructive work as well as dangerous work. The harmful activities are considered as "cyber crime" which includes spamming, credit card fraud, ATM frauds, Money laundering, Phishing, Identity theft, denial of service and other host contributing crime in the Indian Banking sector. This paper has made an attempt to analyze the impact of cyber crime in Indian banking sector.
The study found that cyber crimes are often reduced from the banking transactions by applying the updated technology and appointing reliable officers and devices. This paper is a try to examine the Effects of cyber crime in the Indian banking sector.

INTRODUCTION

Attacks towards the finance industry are becoming increasingly sophisticated and quite focused. Historically, a common (and rather successful) approach of targeting banks has been to direct email phishing at customers. Now, rising channels, which include mobile and online banking, are opening new doors for cybercriminals. To decrease the effectiveness of such attacks, banks have improved each communications to, and the education of, customers, as well as rapidly reacting if an attack occurs. However, criminals have responded not only by creating specialized malicious software designed to compromise online bank accounts, but also by subverting the servers and software owned by professional institutions to enhance the effectiveness of their phishing campaigns; a technique known as infrastructure hijacking.
The Financial Services Information Sharing and Analysis Centre has raised the threat level for attacks from 'elevated' to 'high', citing "recent credible intelligence concerning the potential" for distributed denial-of-service (DDoS) attacks .
This report contains recommendations and satisfactory practices to assist organizations develop a sustainable security infrastructure designed to respond fast to focused on attacks and minimize the consequences of any data breaches.
A criminal offense is an illegal act which isn't to be measured by the issue of occasions, but with the lawful aims and by the bad intentions of fellows. The greatest crime does not emerge from a need of feeling for others however from an over sensibility for ourselves and an over indulgence in our own goals. Cyber crime is a crime committed on the internet. This is a broad term that describes everything from cyber commerce sites to lose money Cyber crime is a digital wrong doing. Any illegal activities committed using a computer or by using the net is known as cyber crime. Digital criminal acts are a variety of wrongdoings, which utilize machines and network systems for criminal exercises.
Cyber crimes can be of different types, for example, Telecommunications Piracy, Cyber Money Laundering and Tax Evasion, Sales and Investment Fraud, Cyber Funds Transfer Fraud etc. The existing current period has replaced the normal financial devices from a paper and metallic based money to plastic cash as a Master

card, credit card, debit card and so forth. This has brought about the increasing utilization of ATM everywhere throughout the sector. The usage of ATM is secure as well as and also convenient. As we all know that every coin has its two side same way in ATM system which is also known as plastic cash is safe and convenient but on the other side which can also be said as the evil side consist of misuse of the same. This wise aspect of the ATM System is reflected as ATM cheats or ATM frauds that is a worldwide burning issue. Cyber crime is rising as a serious threat. Worldwide governments, police departments and intelligence units have commenced to react.

The Information Communication Technology (ICT) has revolutionalized different aspects of human life and has made our lives simpler. It's been applied in exceptional industries and has made business procedures simpler by means of sorting, summarizing, coding, and customizing the procedure. However, ICT has brought unintended consequences in form of different cybercrimes. Cybercrimes have affected different sectors among which banking sector is one of them which have witnessed different forms of cybercrimes like ATM frauds, Phishing, identity theft, Denial of Service.

The human lifestyle has experienced enormous changes every now and then with rapid pace at social level from the earliest starting point and innovative level following the time of ascent of innovations. Banking field is considered one of them. Managing an account tactics to provide facilities and securities to a common man with respect to cash saving Security issues play extremely crucial role in the implementation of technologies specially in banking sector Further on it gets to be primary concerning the virtual security which is at the center of managing an account in banking sector. After the arrival of Internet and WWW this saving money phase has been completely change extraordinarily in respect of security in light of the fact that now cash is in your grasp on a solitary click. Presently client has number of decisions to deal with his cash in distinctive kind of methods. In this paper an endeavor has been made to advance different issues of Indian banks websites for cybercrime safety mechanism and for the security instrument.

CYBER CRIME IN BANKING SECTOR

In today's globalise world to narrow down the world, banking sector provides many facilities to their clients and customers facilities like internet banking, credit card facilities debit card facilities online transfer by this all kind of facilities banks customer can use bank facilities 24 hours and also they can easily transect and easily operate their account from any location of the world with the help of net and mobile. As we all known that as this facilities are useful for the customer but it also have an evil side in which hackers and thefts are protected. They make the misuse of such facilities and by hacking banking sites and customers account make a mess up in accounts and also make a robbery of the money from the customer's account for which the best example was the recent situation in which one of the hacker just take one rupee from the each account but by such one rupee he has collected lots of money.

Banking system is the lifeblood and spine of the economy system. Information Technology has emerge as the spine of the banking system. It gives a excellent aid to the ever –growing challenges and banking requirements. Currently, banks can't think of introducing monetary product without the presence of Information Technology (Reddy.G.N, 2009).Cyber crimes are unlawful activities committed by means of computer end of the criminal activity can be either a computer, network operations. Cyber crimes are genus of crimes, through computers and its networks. Cyber crime is a criminal offense this is committed online in several areas with e-commerce.

Further research on the cyber crime indicates that- it can be categorized in two major ways- (Kumar.A, 2002)

COMPUTER DEVICE USED AS A MEDIUM OF TARGET TO COMMIT CRIME

1. Cyber crime is used as a goal to commit crime in includes
2. Sabotage of computer systems or computer networks
3. Sabotage of operating systems and programmes
4. Theft of data/ information

5. Theft of intellectual property such as computer software
6. Theft of marketing information Blackmail based on information gained from computerized files, such as medical information, personal history, financial data etc

COMPUTER IS WORKING AS AN INSTRUMENT OF THE CRIME

Banking criminals are using various cyber medium which include internet, e-mail, and flash encrypted messages etc to commit crime. This crime via computer network takes place in the banking sector. They are

1. Fraudulent use of Automated Teller Machine (ATMs) cards and accounts
2. Credit card frauds
3. Frauds involving cyber funds transfers (EFTs)
4. Telecommunication frauds
5. Frauds relating to E-commerce and EDI

STATEMENT OF THE PROBLEM

The concept of Cyber Crime is a important aspect. Since a new fact is available in an impartial manner it is often not possible to detect crime on the basis of that information. In the paper, researchers make an attempt to study the Cyber crimes and major crimes of Indian banking sector. In the present globalize scenario, Information Technology is the factor responsible of further growth and development in the Indian banking sector. In this rapid global, customers often feel insecure and reluctant about there banking transactions especially in e-banking or online banking. Technology has emerged as the lifeblood in today Indian Banking sector whether private and public sector banks. Presently, banking sector primarily focus on customer satisfaction the fulfillment of their need and satisfaction in most effective manner. With the advent of "Cyber" within the banking system several problems are emerged as:-

1:-Hacking and stealing of data 2:- Failure of ATMs 3:- Money laundering 4:- Credit card theft

LITERATURE REVIEW

Cybercrime in Banking Sector

Cybercrime according to Douglas and Loader (2000) can be described computer mediated activities conducted via global cyber networks which are either illegal or considered illicit with the aid of certain parties. In the banking sector, the cybercrimes which are committed using online technologies to illegally remove or transfer money to distinctive account are tagged as banking frauds (Wall, 2001). The cybercrimes according to Wall (2001) can be classified into four major categories i.e. cyber-deceptions, cyber-pornography, cyber-violence and cyber-trespass. The banking frauds are sub-classified in cyber-deception which can be defines as an immoral activities such as stealing, credit card fraud, and intellectual property violations (Anderson et al., 2012). There are number of frauds or cybercrimes witnessed in the banking sector, like ATM frauds, Cyber Money Laundering and Credit Card Frauds. However, in general all the frauds are executed with the ultimate goal of gaining access to user s bank account, steal funds and transfer it to few other bank accounts.

In some cases the cyber criminals uses the banking credentials like PIN, password, certificates, etc. to access accounts and steal meager amount of money; whereas in other cases they may want to steal all the money and transfer the funds into mule accounts. Sometimes, the intention of cybercriminals is to just harm the image of the bank and therefore, they block the bank servers so that the clients are unable to access their accounts (Claessens et al., 2002; Hutchinson & Warren, 2003).

As a lot of vulnerabilities exist in the defense system of banking sector, thus there is a need to investigate the ways to increase awareness about the measures that can be undertaken to combat cybercrimes in the banking sector. However, not many studies in the past have been conducted in this area which would suggest ways to mitigate the risks and fight such crimes (Florêncio & Herley, 2011; McCullough & Caelli, 2005).

In order to understand the fraud system in banking sector we will have to understand and describe the attackers and defenders in this environment. The next section therefore describes the different actors which are involved in cybercrimes.

ACTORS OF BANKING FRAUD

The actors of banking fraud can be categorized into four main categories;

Each of these actors and their characteristics have been defined below individually. Cyber Criminals As per the OECD report (2007), these **Malicious Exploiters** can be categorized into five sub categories. Innovators (who are searching security holes in the system to overcome protection measures followed by the banks) Amateur (who are beginners in this area and their expertise is limited to computer skills, which is exploited by the cyber criminal). Insiders (who are working within the bank to leak out important information in order to take some kind of revenge) Copy cats (they are interested in recreating simple tasks). Criminals (highly organized and very knowledgeable who may use all the above mentioned stakeholders for their own earnings).

Money Mules

As per the definition given by OECD report (2007), money mules are people recruited wittingly and often unwittingly by criminals, to facilitate illegal funds transfers from bank accounts. According to the FBI (Federal Bureau of Investigation), these individuals engage in the money transfer activity in exchange of some percentage of that money. According to Florêncio and Herley (2010) there position is to transform reversible traceable transactions into irreversible untraceable ones.

Victims

Victims, according to OECD (2007), in the banking sector can be categorized into two categories; banks and customer of these banks. The users or customers can be individuals, SMEs, or large multinational organizations. The most negative externality most of the valid actors is created by individual users and SMEs who do so by not employing risky online behavior or by not employing security measures during transactions (Asghari, 2010; Mannan & van Oorschot, 2008).

Security Guardians

They are the most crucial actor of this system as they enhance the existing banking system and help in removing the vulnerabilities and improvement of systems so that banking frauds may be mitigated. The security guardians in case of banking sector could be the bank itself or the some third party hired by the bank in order to ensure security from such threats.

IMPACT OF CYBERCRIME ON BANK'S FINANCES

The banking industry across the globe is facing a tough scenario which is thought provoking due to the geopolitical and global macro-economic conditions. The banking sector is forced to assess its current practices in order to analyze and manage their risks effectively. Technology- driven approaches have been adopted for the management of risk. Due to the growth of IT, penetration of mobile networks in normal life, the financial services have extended to masses. Technology has made sure that banking services reach masses as it made these services expensive and accessible (KPMG, 2011).

However, this has also elevated the risk of turning into objectives of cyber attacks. Cybercriminals have developed advanced strategies to not only cause theft of finances and finances information but also to espionage businesses and access important business information which indirect impacts the bank s finances. Globally, USD 114 Billion is lost nearly every year because of cybercrimes, and the cost spend to combat cybercrimes is double is amount i.e. USD 274 billion (Symantec Cyber Crime Report, 2012).

On an average, banking facilities take 10 days to fully recover from a cyber act which further adds to the cost of operation. Comparing the financial losses faced by the Indian Banking Sector, it is nearly 3.5% of the loss in cash in comparison to global loss. USD 4 billion is lost in recovering from the crime and USD 3.6 billion is spent to combat such crimes from happening in future. The average time taken to resolve the crime in Indian banking sector is also higher in comparison to global scenario i.e. 15 days (Muthukumaran B., 2008).

In order to fight these cybercrimes, the banking sector needs to collaborate with global authorities and watchdog organizations so that a model can be developed which can help in controlling and dealing with such threats. The main issue of concern here is that there is absence of effective compilation service in the banking sector which can identify the trends in cyber-crime and compile a model according to it. However, in the last few months, banks all across the globe have perceived cybercrime as among their top five risks (Stafford, 2013).

High profile banks in the UK like Barclays and Santander were targeted by hackers who stole personal information of nearly 2.9 million credit card customers by hacking the software maker system of these banks, which led them to incur huge losses. However, the scenario is not restricted to UK, in US as well such attacks have surfaced in the past years and in order to curb the affect, they launched the program Quantum Dawn 2 which test the efficacy of system installed in banks in response to cyber-attacks (Stafford, 2013).

However, the sad truth is that most the systems are one-step behind the tools adopted by cyber criminals which has resulted in demand of development of system which is flexible is meeting and destroying the incoming assaults. A solid defense system to resolve attack is the need of the hour before, during and after the attack.

TYPES OF CYBER CRIME IN BANKING SECTOR

1) ***Hacking*:-** "Hacking" is a crime, which means an unauthorized access made by a person to cracking the systems or an attempt to bypass the security mechanisms, by hacking the banking sites or accounts of the customers. The Hacking is not defined in the amended IT Act, 2000. But under Section 43(a) read with section 66 of Information Technology (Amendment) Act, 2008 and Section 379 & 406 of Indian Penal Code, 1860 a person or a hacker can be punished. If such crime is proved then for such hacking offence the accuse is punished under IT Act, for imprisonment, which may extend to three years or with fine, which may be extended to five lakh rupees or both. Hacking offence is considered as a cognizable offence, it also a boilable offence.
2) ***Credit Card Fraud*:-** There are many online credit card fraud are made when a customer use their credit card or debit card for any online payment, a person who had a mala fide intention use such cards detail and password by hacking and make misuse of it for online purchase for which the customers card used or hacked is suffered for such kind of attract or action of a fraud made by and evil . If cyber transactions are not secured the credit card numbers can be stolen by the hackers who can misuse this card by impersonating the credit card owner.
3) ***Email Fraud*:-** In present period of life e-mail and websites are become a speedy, easy and preferred means of communication. some times by email fraud is made some of the hacker or a evil organization send email to bank customers that "congratulation you have won such a huge amount to enchase it please share your bank details" and by such customer simply have to type credit card number into www page off the vendor for online transaction or for enchase of such kind of amount then hacker make a miss use of such detail and make a crime which is also known as cyber crime as per law.

4) ***Phishing*:-** Phishing is only one of the numerous frauds on the Internet, attempting to trick individuals into separating with their cash. Phishing alludes to the receipt of spontaneous messages by customers of financial institutions, asking for them to enter their username, secret word or other individual data to access their account for some reason. customers are directed to give a response to a mail and also directed to click on the link mentioned in the mail when they click on the given link for entering their information which were asked in the mail received by the fraudulent institution's of banking website, by such kind of activities customers thus they remain unaware that the fraud has happened with them. The fraudster then has admittance to the client's online financial balance available in the bank account and to the funds contained in that account by making the misuse of the detail received from the customer fraudulently. F-Secure Corporation's outline of 'information security' dangers amid the first 50% of 2007 has uncovered that the study discovered the banking industry as vulnerable objective for phishing tricks in India
5) ***Financial Fraud*:-** Financial Fraud in UK, an industry body, says British misfortunes from web and phone managing account extortion climbed 59 for every penny to £35.9m in the initial six months of the year. It says that reports of fishing attacks indicate it is one of the quickest developing sorts of extortion. In response the banks have called for UK telecom groups to reduce the time people can stay on the line after someone else hangs up. By next year, most telecom operators will have cut the disconnection time to two seconds. Accordingly the banks have called for UK telecom groups to reduce the time individuals can stay hanging before anyone else hangs up. By one year from now, most te Phishing is one and only illustration of the continually developing digital risk that banks and their client's face, which is the reason the issue, has vaulted on to the motivation for sheets of executives, controllers and law authorization organizations.
6) ***Cyber Security***:- Specialists say banks confront four wide sorts of risk. First, country and states use surveillance to both, take intellectual capital from banks and to destabilize them. Secondly, banks are a prime focus for cyber terrorists looking to strike against images of western capitalism. Third, purported "hacktivists" consistently make crafty endeavors to break into banks' IT organizes, normally to win more attention for their reason. At long last, sorted out wrongdoing has to a great extent moved from taking cash through conventional bank heists to utilizing different means, for example, on the web, phone and card misrepresentation, which are harder to identify.

CURRENTLY ADOPTED SECURITY MODELS

The models currently adopted in online banking systems are based on several security layers, consisting on diverse parallel solutions and mechanisms which aim at protecting the banking application and the user's data, providing identification, authentication and authorization.

• Digital Certificates: Digital certificates are used to authenticate both the users and the banking system itself. This kind of authentication depends on the existence of a Public Key Infrastructure (PKI) and a Certificate Authority (CA), which represents a trusted third-party who signs the certificates attesting their validity. In Brazil, banking systems use A1 and A3 certificates issued and signed by ICP-Brasil .

• One-Time Password Tokens: One-Time Password devices are commonly used as a second authentication factor, which may be requested in specific or random situations. This kind of devices render captured authentication data useless for future attacks through the use of dynamically changing passwords which can be used only once.

• One-Time Password Cards: One-Time Password Cards constitute a less expensive method for generating dynamic passwords, also providing a second authentication factor. However, in some banking systems, passwords generated by OTP cards are reused a number of times before being discarded, rendering this system vulnerable to short term replay attacks.

• Browser Protection: In this model, the system is secured at the Internet browser level, which is used to access the banking system. The user and his browser are protected against known malware by monitoring the

memory area allocated by the browser in order to detect such malware and hinder credential theft and capturing of sensitive information.

• Virtual Keyboards: Virtual keyboards were developed to thwart the efficient use of keyloggers (which capture information typed into the device). These devices are usually based on Java and software based cryptography, allowing portability between different devices. Currently they are being replaced by other more efficient methods which require less processing power and slower transmission rates.

• Device Registering: This method restricts access to the banking system to previously known and registered devices. Hardware fingerprinting techniques are used in conjunction with user identification through secret credentials.

• CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart , is a method recently adopted in some banking systems whose objective is to render automated attacks against authenticated sessions ineffective. This method requires the legitimate user to input information conveyed as scrambled images which are difficult for automated robots to process and recognize.

• Short Message Service (SMS): This method has been applied in some banking systems to notify users about transactions requiring their authorization. It provides a second authentication channel for transactions that fit certain characteristics by sending to the user a set of characters which have to informed in order to authorize and process the transaction through the online banking system.

• Device Identification: Device identification is usually applied together with device registering but it is also used as a stand-alone solution in online banking systems that aim at facilitating user access. This identification model is based on physical characteristics of the user's device through which it is possible to identify its origin and history information.

• Positive Identification: Positive identification is a model where the user is required to input some secret information only known to him in order to identify him. It is applied as a second authentication method.

• Pass-Phrase: It is a security model based on information held by the user. It is usually used as a second authentication method in transaction that involves money movement.

• Transaction Monitoring: Even though this method is not thoroughly analyzed in the present work, it is currently applied in all online banking systems, each of them using different techniques. Artificial intelligence, transaction history analysis and other methods that identify fraud patterns in previously processed transactions are among the various approaches to transaction monitoring.

IMPLEMENTING BEST PRACTICES AGAINST TARGETED ATTACKS

There are a number of key issues that financial institutions should consider in order to move beyond a one-size-fits-all approach and begin to successfully fight targeted attacks.

1. ***Predictive Threat Analysis***

   Threat intelligence is a key starting point for any enhanced security strategy. Before selecting an information security tool, institutions should identify their core business processes, classify the information they handle, understand how data flows, comprehend the legal and regulatory landscape they exist within, and then adopt a risk-based approach to setting priorities. By identifying assets, threats and vulnerabilities, this approach allows the qualification and quantification of probable occurrence and impact.

2. ***Employee Training***

   Due to the extensive list of information security domains, some organizations focus mainly on initiatives around governance: risk and compliance; identity management and access control; data loss prevention; network and information security; and penetration testing. While these five domains set the foundation for information security, organizations should not forget that security processes, tools and infrastructure are defined and supported by people, not machines. Thus, effective awareness programmes and well-trained staff are crucial to cyber security solutions. An internal security task team should work with a trusted security vendor to perform a detailed analysis of risk management.

Organizations do not need to hold all the expertise in-house, as specialist skills can be acquired from trusted organizations as required.

3. ***Identity Management***

The key to protecting customer information is establishing a stringent identity management programmes that implements multi-factor authentication; strong data encryption mechanisms to protect data storage and transmission; and fraud detection and monitoring mechanisms. In addition, when mobile devices are part of the strategy, all associated threats must be identified before granting consumer access to sensitive functions and data.

4. ***Measurement And Reporting***

Constructing a well-established metrics programme to effectively analyse the cost-benefit ratio of security solutions is paramount, as it will allow CISOs to articulate the value of security solutions. The cost associated with the security solution can then be compared with the cost associated with the data, assets and overall value in need of protection, thus ensuring the solution does not exceed this value.

5. ***Test Your Plan***

Test your plan before a breach happens. Security intelligence should enable breaches to be discovered rapidly and stopped at an early stage. Processes and tools, such as backup and data loss prevention, should also be available to recover and restore information.

REASONS FOR CYBER CRIME

Computers are exposed, therefore, the law is mandatory to protect and safeguard them against cyber crime or electronic crime in Indian banking sector. Mostly researchers research in cyber crime victims arise in banking activities through e-services. The reasons for the exposure of computers may as follows:

- ***Competence to Accumulate Data*:** The computer has exclusive characteristic of storing data in a very comparatively small space this makes the user more comfortable to steal the data either physically or virtually through any electronic medium in their banking sector. If there is not updating use softwares & antivirus etc.
- ***Lack Of Legislation Laws*:-** Analysis of the legislative exercise of law and policy formulation in the field of cyber crime legislation, revealing quite emphatically the need for carefully worded provisions, foresight in the drafting process and imagination with respect to explanations to particular sections.
- ***Issue of Cyber Security*:-**Capacity includes having comprehensive national Banking and policies, cooperation, skills and workforce, technology and expertise to tackle online threats and reduce harm, while ensuring cyberspace supports innovation, economic growth and social benefits in Indian banks.
- ***Unproblematic to Approach:*** The trouble encountered in guarding a computer system from unauthorized access is that there is every opportunity of breach due to the complex technology in Indian banking sector. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.
- ***Complex:*** The computers effort on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.
- ***Negligence:*** Negligence is directly associated with human behavior. While protecting the computer system it is possible there might be any negligence, which change direction provides of the cyber criminal to gain access and control over the computer system.

CONCLUSION

The paper gives a brief overview of cybercrime scenario in the banking sector and impact of cybercrimes on bank finances. The major cybercrimes which plague the banking sector are ATM frauds, Denial of Service, Credit Card frauds, phishing, etc. The rapid growth to global cyber crime and the complexity of its investigation requires a global presence. Presently, the measures undertaken the banks are not sufficient and therefore it is imperative to increase cooperation among the banks across the world for the development of tools and models which can be applied to counter global banking cybercrimes.

Credit card fraud can be devoted using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction. The reason may be to obtain goods without paying, or to obtain unauthorized funds from an account. The regulatory framework must also take into account all the related issues like development of e-money, right to privacy of individual. International law and international co-operation will go a long way in this regard. At last it can be concluded that to eliminate cyber crime from the cyber space is not a possible task but it is possible to have a regular check on banking activities and transactions. The only promising step is to create awareness among people about their rights and duties and further making the application of the laws more stringent to check crime. There is a need to bring changes in the Information Technology Act to make it more effective to combat cyber crime

REFERENCES

1. U.S. Financial Sector has raised its Cyber Threat Level from Elevated to High, 21 September 2012 http://cyberwarzone.com/us-financial-sector-hasraised-its-cyber-threat-level-elevated-high
2. www.ijcrar.com_vol-2-2_A.R. Raghavan and Latha Parthiban
3. Types of Cyber Crimes & Cyber Law in India, Available at http:/ / www. csiindia.org /c/document_library/get_file?uuid=047c826d-171c-49dc-b71b-4b434c5919b6, Last visited (30/4/2015)
4. Cyber law and Crimes: by Barkha Bhasin, Rama Mohan Ukkalam
5. http://resources.infosecinstitute.com/modern-online-banking-cyber-crime/, Last visited (20/1/2015)
6. Articles on ITA 2008
7. Articles on IT Act 2000 & IT Rules 2011
8. Cyber Law Cyber Crime Internet and E-Commerce by Prof. Vimlendu Tayal
9. Alaganandam, H., Mittal, P., Singh, A., & Fleizach, C. 2007. Cybercriminal Activity.
10. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. 2012. Measuring the cost of cybercrime.
11. Asghari, H. 2010. Botnet mitigation and the role of ISPs: A quantitative study into the role and incentives of Internet Service Providers in combating botnet propagation and activity. Delft University of Technology.
12. Böhme, R., & Moore, T. 2009. The Iterated Weakest Link--A Model of Adaptive Security Investment.
13. BhasinM (2007). "Mitigating Cyber Threats to Banking Industry" , The Chartered Accountant, April 2007, p.1622-1623
14. Choo.K.K.R (2008). "Money Laundering risks of prepaid stored value cards" ,Australian Institute of Criminology, September, No.363, pp. 1-6
15. Choo, K.-K. R. 2011. The cyber threat landscape: Challenges and future research directions. Computers & Security, 308: 719-731.
16. Claessens, J., Dem, V., De Cock, D., Preneel, B., & Vandewalle, J. 2002. On the security of today s online cyber banking systems. Computers & Security, 213: 253-265.
17. Douglas, T., & Loader, B. D. 2000. Cybercrime: Security and surveillance in the information age: Routledge.
18. Florêncio, D., & Herley, C. 2010. Phishing and money mules. In Information Forensics and Security WIFS, IEEE International Workshop on pp. 1-5. IEEE.
19. Florêncio, D., & Herley, C. 2011. Where Do All The Attacks Go? Economics of Information Security and Privacy III pp. 13-33. Springer New York.
20. Hutchinson, D., & Warren, M. 2003. Security for internet banking: a framework. Logistics Information Management, 161: 64-73.
21. Jaleshgari, R. 1999. Document trading online. Information Week, 755: 136.
22. KPMG 2012 [Online] Cybercrimes: A Financial Sector Review. Government and Public Sector. Available at: https://www.kpmg.com/in/en/industry/p ublications/fs_cybercrime_booklet.pdf
23. Mannan, M., & van Oorschot, P. C. 2008. Security and usability: the gap in real- world online banking. Paper presented at the Proceedings of the 2007 Workshop on New Security Paradigms.

24. McCullagh, A., & Caelli, W. 2005. Who goes there? Internet banking: A matter of risk and reward. Paper presented at the Information Security and Privacy.
25. Muthukumaran. B 2008. Cyber Crime Scenario in India, Criminal Investigation Department Review, pp.17-23
26. OECD. 2007. Malicious Software Malware: A Security Threat to the Internet Economy.
27. Premchaiswadi, N., Williams, J. G., & Premchaiswadi, W. 2009. A Study of an On-Line Credit Card Payment Processing and Fraud Prevention for e- Business. In T. Bastiaens, J. Dron, & C. Xin Eds., World Conference on E- Learning in Corporate, Government, Healthcare, and Higher Education 2009: 2199-2206. Vancouver, Canada: AACE.
28. Reddy.G.N, (2009). "IT- Based Banking Services Enhancing Efficiency" , Financial Analyst, November,p.69
29. Sherstobitoff, R. 2013. Inside the World of the Citadel Trojan McAfee Labs. Stafford P. 2013 [Online] Cyber crime threatens global financial system. Available at: http://www.ft.com/cms /s/0/9804988c-3722-11e3-9603-00144feab7de.html#axzz2tMwSTsmF.
30. Symantec Cyber Crime Report, 2012 [Online] Cybercrime Report. Available at: http://now-static.norton.com /now/ en /pu/images /Promotions /2012/ cybercrimeReport/2012_Norton_Cyber crime_Report_Master_FINAL_050912. pdf
31. TrendMicro. 2013. Security Threats to Business, the Digital Lifestyle, and the Cloud.
32. Vrancianu, M., & Popa, L. A. 2010. Considerations Regarding the Security and Protection of E-Banking Services Consumers Interests. The Amfiteatru Economic Journal, 1228: 388-403.
33. Wall, D. 2001. 1 Cybercrimes and the Internet. Crime and the Internet: