JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Impact of Cyber Crime on the Banking Sector

Pankaj Sareen
Assistant Professor, Swami Premanand Mahavidyalaya, Mukerian
pankaj.sareen1480@gmail.com

Dr. Pallvi Rani
Assistant Professor, Mehr Chand Mahajan DAV College for Women, Chandigarh
pallvidhingra06@gmail.com

Abstract: The banking sector is now being improved and made stronger by online banking to attract its customers these days still most banking customers do not use net banking due to fear of cyber crimes. This research tries to aware the readers to know the meaning; types of cyber crimes and cybercrime laws. The risk of cyber-attacks has increased over the world with ICT. There is a need to explore this area as the various attacks like the stealing of information, hacking, and viruses, are increasing day by day. Banks must evaluate their current policies as although the number of customers in the banking sector has increased yet they feel hesitant and unconfident in selecting online services. This Paper attempts to study the impact of cybercrime on the banking sector. The security recommendations are highlighted in this study so that the knowledge level of online banking account holders can be improved when dealing with online attacks. This research will also be beneficial for financial organizations and banking sectors. The uniqueness of this paper is based on the inclusive methodology used to know the types of online attacks and their prevention.

Keywords: Cyber Crimes, Phishing, Vishing, Identity Theft, Cyber Crime Prevention, RBI Guidelines.

I. Introduction to cybercrime in the Banking sector

ICT which is also known as Information and Communications Technology can now be seen in almost every area of life. People are now using this technology for online transactions like sending money and making online payments. There is no doubt that this technology has made a full impact on banking services. We should not forget that cyber threat is a deep concern if we want to use online transactions. We can see many cases of fake cash withdrawals, hacking of accounts; theft of data; and numerous scams related to debit/credit cards. As maximum information is available online these days, it is highly prone to various attacks by criminals, and such type of fraud cases now becoming more common so account holders have a massive loss of cash year by year.

It may be strange people that no cases of cyber crime related to online banking were reported before 2014[1] even though people have been using Online transactions since 1981. According to the study, after this period, there was a swift boost in the efforts made to acquire unauthorized access to steal records of customers by cyber attackers. According to a study [2], the approximate yearly cost of cybercrime is $100 billion all over the world [3]. Keeping this in mind, it is very important to spread awareness about different types of cyber attacks in the banking sector. Any Crime that involves the use of ICT as a medium is known as a cyber attack [4] which is considered a high risk to a nation's economic growth in all aspects as financial institutions are now victims of the attack [5]. There are two categories of cybercrime: Devices used as a medium of target; Computers working as an instrument of the crime [6]. One of the most severe attacks in net banking is phishing in which the attacker uses social engineering techniques to deceitfully obtain susceptible information, such as credit/debit card details, usernames, passwords, etc. by masquerading as a reliable entity [7].

II. Problem Statement

The banking sector is now being improved and made stronger by online banking to attract its customers these days still most banking customers do not use net banking due to fear of cyber crimes. This research tries to aware the readers to know the meaning; types of cyber crimes and cybercrime laws. The risk of cyber-attacks has increased over the world with ICT. There is a need to explore this area as the various attacks like the stealing of information, hacking, and viruses, are increasing day by day. Banks must evaluate their current policies as although the number of customers in the banking sector has increased yet they feel hesitant and unconfident in selecting online services. This Paper attempts to study the impact of cybercrime on the banking sector

Need and significance of the study

The security recommendations are highlighted in this study so that the knowledge level of online banking account holders can be improved when dealing with online attacks. This research will also be beneficial for financial organizations and banking sectors. The uniqueness of this paper is based on the inclusive methodology used to know the types of online attacks and their prevention.

Objectives of the Study:

The current study aims:

- To know and understand the concept of cybercrime and its categories and its impact on the banking sector.
- To examine and use the precautionary actions available to control fraud.
- To highlight some of the cyber crimes that happened in 2018-19 so that online banking users can be made aware
- To review RBI's new guidelines for customers against cyber fraud.
- To suggest preventive measures and safety tips to control and prevention of cyber-crimes

III. The Literature Review

Nappinai N. S. (2010) in his research has shown important terms of the criminal laws in India relating to information safety, confidentiality, and other computer-generated offenses.

Ashwini B. (2012) talked about generally the rate of growing online crimes with their adverse effect on online banking. The legislative actions to stop cybercrime and the challenges that the Country needs to look to control cyber threats were also discussed.

Susheel B. and Durgesh P. (2011) in their paper highlighted that protection plays an important role in the banking sector as money is just simply only click away. Different issues faced by the Indian banking system face and the need for cyber security were also discussed.

Sanjay P. (2010) has made an effort to investigate the existing trends in cybercrime and analyzed the needs of legislation and recent provisions of the IT Act by discussing similar provisions in the world.

Mani A. (2012) tried to explore the causes of cybercrime activities and the effect of these activities on the growth and development of the E-commerce industry. The author further concluded with various tips to deal with cyber crimes.

Cezar V. (2012) suggests that particular concentration should be given to clearly distinguish between cyber war, cyber attacks, and cyber terrorism, and the process for the accomplishment of the nation's public cyber response operations should be maintained.

Mohit G. (2012) concentrates on cyber ethics and focuses on other countries' policies and rules. He then highlighted that education and awareness must be given to citizens of India so that unlawful activities can be minimized. Steps that must be taken by the Indian government to control these criminal activities were also focused on.

Hemraj S. & Panda T.C. (2012) in their study described in depth the cybercrime impact on various sections of society [8].

Singh B. (2013) in his report observed that as there are few numbers of cyber law firms in India so the maximum numbers of these crimes are not even reported.

Poonia A. (2014) has given the insight to understand the classification of cybercrime and its challenges in the International Journal of Emerging Trends and Technology in Computer Science [10],

Yatindra S. (2010) described that with time, the banking system has many changes with the adoption of ICT [11]. Various rules, copyrights, & their subsistence in the cyber world were also discussed by the Author.

Sood V. (2010) has described the characteristics and types of cyber crimes and recommended various methods to control cyber crimes [12]. He added that online crimes cannot be fought on an individual basis and nations must come together to counter these crimes

Harish Chander (2012) described the International Efforts relating to Cyberspace Laws and Cyber Crimes [13]. The author commented upon the Penalties, recompense, and resolution of infringement of provisions of IT and legal examination.

Shamsul H. & Mustafa B. (2013) commented that banks are now spending a great deal on ICT but from the government side also there is need to invest in internet security [14].

Uppal R.K. (2011) highlighted the merits of net banking and suggests some measures to spread awareness regarding E-banking and to increase its area and scope to enhance net banking services in rural and semi-urban areas [15].

Jyoti Ranjan H. (2013) concluded that there are many challenges related to security issues of software installed in ATMs [16].

Abhimanyu (2010) first classified the various types of cyber crimes based on the offense committed [17]. He suggested that cyber cells shall be formed in all the police stations throughout the country and training about cyber laws must be given to everyone related.

IV. Types of cyber crimes in Banking

Phishing: It is a method to acquire confidential data, for example, usernames, and passwords by acting as a reliable entity [18]. There are numerous tricks used by attackers: one is sending phishing electronic mail to banking account holders by acting like an authentic group is providing services. Spoofing sites can also be used in which criminals design similar websites to the original website which can steal data [19].

Vishing: It is the illegal activity in which individual information is obtained with regards to utilizing social designing via phone framework and budgetary data with the end goal of monetary reward [20].

Identity Theft*:* It is the method by which a person's information such as birth date, name, etc. is acquired by fraudsters, and then any vital purpose such as obtaining a credit card or loan is obtained later from this information.

Credit Card Fraud: In this, credit card data is stolen by the criminal and then he can use this to make online transactions when transactions are not properly protected.

Keystroke logging: It is another kind of method in which criminals attack the victim's computer and record the keystrokes with the help of Key loggers which are Trojan software programs. It is severely harmful as hackers can have access to any information like user ID, password, account number, and anything typed.

Malware*:* Cyber criminals can steal sensitive information by spreading Viruses, Worms, Trojans, etc. which are known as Malware. Malware growth is tremendous over the last few years because of the rapid growth in mobile devices. Thousands of frauds against online consumers are recorded to obtain a huge amount of money illegally in online banking by malware applications. Most mobile operating systems like Android are now victims of malware attacks so it is significant to consider this [21].

Automating Online Banking Fraud*:* This is another type of attack in which criminals hack the online accounts of customers and every month they steal few amount of money that is even not noticed by the customer. Criminals have developed a new system for this known as the Automatic Transfer System [22].

Denials of Service (Dos): Denial of Service means to make a network resource unavailable to its users. In such types of attacks, the attacker sends many requests in a short period to a legitimate server the server becomes busy responding to replies and its service becomes unavailable to the users. The most harmful is Distributed Denial of Service in which the attacker sends requests not from a single system but from a network of systems [23]. The impact of such attacks is significant [24].

Watering hole: "Watering hole" cyber fraud is considered to be a branch arising from phishing attacks. In this method a harmful code is inserted onto web pages that are visited only by a small group of people then the information of the victim can be traced.

V. Cases of Cyber Crimes in the Online Banking Sector

Customers of US banks faced theft of their payment card data by various Vishing attacks. Customers received an SMS that their debit card has been deactivated and if they want to reactivate it then provide the details of the card and PIN [25].

In Umashankar Sivasubramanian v. ICICI Bank case [26], the sufferer used to get bank account statements monthly from the bank's e-mail. He provided personal details when asked by e-mail and his account was debited with Rs. 5 lacs. He then approached adjudicating officer when Bank told him that it was a phishing email. In this case, according to Section Forty-Three and Section Eight Five of the IT Act, 2000, the Bank was held responsible as the Bank failed to provide adequate checks and safeguards to prevent unauthorized access to the customer's account [27]

A management trainee of the bank was engaged to be married in the Bank NSP case [28]. Many e-mails were exchanged between the couple using the computers of the company. A girl created false email ids and sent many e-mails to the clients of the husband by using the bank's computer when they were not in a relationship after some time. Many customers were lost by the boy's company so they approached the court against the Bank and then the Bank was held responsible because emails were sent from the Bank's system.

In case of any fraud on customers on the bank, there is a burden of proof laid down on the bank- this statement was held by the court in the case of the Manager of Axis bank ltd vs. Sai Sandeep [29].

Incidents of Cyber Crime in Banking in 2018-19

Hackers steal Cosmos Bank's ATM Card Data and withdraw Rs. 94 crores: About 100 Crore was stolen by the hackers from the server of the Cosmos Bank in Pune [30]. Hackers acquired the details of many Visa and Rupay debit cards to make around ten thousand illegal transactions worth Rs. Eight Crores and three thousand transactions worth Rs. Fifteen crores.

Extensive fraud on Amazon: According to a UK legal document a serious online attack that took place between May-October 2018 was made on the hundred accounts [31] of Amazon by hackers who transfer money to their accounts from loans or sales between May 2018 and October 2018.

Over 5 Billion Dollars from Crypto Crimes stolen by hackers Last Year: According to a study from CipherTrace [32], a cryptocurrency firm, 2019 which publishes reports on cryptocurrency thefts, scams, and fraud worldwide, criminals and fraudsters netted approximately $4.26 billion for the first half of the year. According to the report, cryptocurrency thefts reached $1.2 billion in the first quarter of 2019 and $1.7 billion for the year 2018. Most of the incidents involved attacks in which hackers employ multiple techniques- including SIM swapping, phishing, URL hijacking, etc. against multiple targets to take over user and administrator accounts. Users were not able to receive alerts because of the SIM Swapping so they were unaware of these highly unusual transfers.

Punjab CM's wife Preneet Kaur was cheated by the Jharkhand man: Preneet Kaur, wife of Punjab's Chief Minister Captain Amarinder Singh was looted as the group from Jharkhand took about Rs. Twenty-Five lacs from her account. The mastermind Ataul Ansari called up Preneet Kaur when she was attending the Parliament. Masquerading as a State Bank of India (SBI) manager, Ataul asked for the ATM PIN and OTP number from Preneet Kaur. He told Preneet that her salary has to be credited to the account and that vital information is needed immediately. After securing the PIN and OTP, Rs 23 lakh was withdrawn from Preneet Kaur's account in three transactions [33].

6 Hackers Linked to DDoS and Financial Attacks were arrested by Ukrainian Police: Hackers were seized by the police who were involved in carrying out Distributed Denial of Service attacks against news agencies [34]. They first attacked computers, infected them with Trojan malware, and then enabled key-logging to acquire vital information while information is provided using these computers and then transferred money to their accounts.

Advertising partners of various E-Commerce sites infected by hackers: RiskIQ and Trend Micro Researchers revealed that cybercriminals of a new subgroup of Magecart in recent times effectively attacked around 300 Online Shopping websites with the help of supply-chain attacks [35]. Hackers silently acquire the payment information of customers while they purchase the checkout page of sites by inserting malicious JavaScript code.

Developer Stole Bitcoins: Developers infected the most commonly used third-party NodeJS module with harmful code which was coded to obtain money stored in a Bitcoin wallet [36]. The malicious code attempted to steal digital coins stored in Dash Copay Bitcoin wallets.

Credit Card Information was stolen by Hackers From Electronics Retailer: According to RiskIQ, Magecart hacking group stole the information on the credit card of all the customers by inserting malicious programs into the payment processor web page between August 14 and September 18, 2018[37]. The group first purchased a web domain "neweggstats.com" because it was similar to Electronic Retailer's original web page "newegg.com" and then inserted a

malicious program in an original website which was used to obtain credit card information when the user provided the details and this information is sent to "neweggstats.com" webpage.

Bank Servers Hacked to Trick ATMs into Spitting Out Millions in Cash:

The US-CERT researchers found ten malware related to FAST cash cyber crimes which were used to attack the servers of banks which are used to validate user accounts to perform illegal transactions. The malware fooled ATMs to dispense money without notifying the bank [38].

VI. Preventive Measures and Suggestions to Control Cyber Crime Frauds

Strategic national measures to combat cybercrime: Managing an account segment is the foundation of our economy. The expanding number of digital wrongdoing cases has brought about gigantic losses to our economy. Both the banks and the client must know about various hazards and shield measures. There should be a collaboration between the different partners to counter anything wrong. The Government should ensure some national measures to combat crimes [39].

Committee to deal with Online Frauds: There must be a committee in every bank that must deal with cyber frauds and in case that committee does not perform its duty the same must be reported [40].

Customer Awareness: The bank customers must be instructed about various cheats and counters. A client ought to be made mindful of the Rules and regulations of E-managing an account. It very well may be done through notifying it on the Bank's site, papers, notices, SMS, and training [41]. The proper training should be provided to the customer and it should be updated if in case there is any change [42]

Strong Methods of Cryptography: There must be strong Cryptography methods that will be used while making online transactions so that information must be connected in an encrypted manner and security can be assured [43].

Physical Security of ATMs: Physical Security of ATMs is also very important because there are many incidents happened where ATMs are plundered [45].

Cooperation among Nations to Avert Cyber Crime: Dealing with cyber crimes is not a task of only one country. All the nations must come together. India can take the help of other countries to counter cyber crimes by following their policies.

In Addition to the above, the common security measures that must be known by banking users are listed below:-

Device Security: The security of the devices like computer systems, mobile, etc. used for net banking access is important.

Protection of Personal Data: You should not share precious data with anyone. You must know the reason and take measures to avoid any trick used by attackers while providing information.

Use Strong Passwords: Online users should use a strong password which is a combination of different alphabets, special characters, and numbers. If your password is not strong it can be guessed or cracked very easily by fraudsters. Passwords should not be written down anywhere.

Be Secure when Online*:* The user should regularly check the security settings of his account and proper care should be there that any private important information should not be disclosed. The following points must be considered in mind:-

- You should not use online banking, E-Commerce website, etc. if you think that the internet you are using is not properly secured.
- Sometimes, you may get some phishing E-mails from the attackers so you should not follow any link by clicking.
- To avoid any clicking by mistake, you should immediately delete any spam E-mail.
- An attacker can offer you prizes in terms of lotteries you should not call on the numbers that are provided in these messages and you should never respond to these messages.
- Your credit card information can be used by the attackers so never provide a Xerox copy of the card to anyone.

- Regularly check the monthly credit statement of your account and if in case, you do not receive it you should immediately inform the bank. Also, inform the bank if your credit/debit card is misplaced or lost.
- You must not disclose your credentials to anyone either in public or through SMS

Upgrade your System and Software: You should continuously upgrade your system and software so that any security breach can be avoided.

Suggestions to control cyber crime frauds:

- An act has to be enforced because the major impact of cyber crimes is left unsolved a large number of times as currently there is no specific enforcement related to the cyber laws.
- Law enforcement should be very firm and reorganized from time to time to keep a track of such crimes.
- To solve the cases and boost trust among people, there should be fast-track mobile courts
- Cyber Attackers must be given proper punishment so that impact of cyber crimes can be minimized.
- People should be given proper awareness regarding cyber threats, and precautionary measures through different awareness programs.
- The public must report any cybercrime case to not only the bank but also to cybercrime branches for fast and strict action.

New Guidelines of RBI for Bank Account holders against any Cyber Crime: According to new guidelines, the banks will have to compensate the customer if there is a fault of the banks and if there is a third party fault then Banks will compensate account holders as per their customer relations policy[46]. For making E-payments safe for the people, RBI has a concept of no liability and limited liability in which if any illegal transaction is reported by the customer within three days, account holders will not suffer any loss and within ten days, the same amount will be credited to their accounts. Here are the final guidelines [47] sought to make the online transaction safe.

- A new concept of zero liability and limited liability in which if any illegal transaction is reported by the customer within three days, customers will not suffer any loss
- Within ten working days from the date of any unauthorized transaction reported by the user, the bank has to credit the amount involved to the customer's account.
- The customer will bear the entire loss if a customer is responsible for any unauthorized transaction (suppose the customer has shared his password due to negligence) and has not reported this to the bank.
- The maximum liability of the customer will be Rs. Five thousand to Rs. Twenty Five Thousand which depends on the type of account if any fraud transaction is notified within four to seven days.
- The customer liability will be according to the bank's policy if any fraud is reported after 7 days.
- The transactions include internet banking and mobile banking as well as ATM and point-of-sales transactions.
- The complaint form must be available on the bank's website for filing complaints.
- All account holders of the bank must be registered for SMS and E-mail alerts compulsory and customers should be able to reply in case of any cyber attack.

VII. Conclusion

ICT which is also known as Information and Communications Technology can now be seen in almost every area of life. People are now using this technology for online transactions like sending money and making online payments. There is no doubt that this technology has made a full impact on banking services. We should not forget that cyber threat is a deep concern if we want to use online transactions. We can see many cases of fake cash withdrawals, hacking of accounts; theft of data; and numerous scams related to debit/credit cards. As maximum information is available online these days, it is highly prone to various attacks by criminals, and such type of fraud cases now becoming more common so account holders have a massive loss of cash year by year. So, it is very important to aware online banking users of various cyber threats and their prevention. So this paper has discussed the various cyber-attacks along with various safety measures. The various cyber attacks that have been reported last year were also included in this research. Banks and RBI must issue various safety measures from time to time. This Paper also concluded the new RBI Guidelines that are available for Bank account holders against any cybercrime.

References

[1]. Sia, P. (2013). Online banking and fraud: A new generation of cybercriminals, finance, and strategy. The Financial Service Blog of Sia Partners.
[2]. GoGolf. (2013). Cybercrime statistics and trends. Retrieved from the website: http://www.go-gulf.com/blog/cyber-crime/
[3]. Kirsty. (2015). Cybercrime, one of the biggest Middle East security threats. Retrieved from the website: http://securitymiddleeast.com/2015/01/05/cybercrime-one-biggest-middle-east-security-threats/

[4]. Kharouni, L. (2012). Automating Online Banking Fraud Automatic Transfer System: The Latest Cybercrime Toolkit Feature (Rep.).
[5]. www.cyberlawsindia.com
[6]. Kumar. A (2002) "cyber crime- crime without punishment", available at unpanl.un.org.
[7]. Perumal, Subramaniam Arumuga, Impact of cybercrime on virtual banking (oct 24,2008) available at www.ssrn.com
[8]. Saini Hemraj, Rao Yerra Shankar and Panda T.C., CyberCrimes and their Impacts: A Review', IJERA, 2(2), 202-209 (2012)
[9]. Singh B., Online Banking Frauds In India, Report, Retrieved from http://perry4law.org
[10]. Ajeet Singh Poonia, cybercrime, challenges and its classification, International Journal of Emerging Trends and Technology in Computer Science (Volume 3, issue 6, Nov- Dec 2014, pg 120)
[11]. Singh Yatindra Justice, Cyber Laws, Universal Law Publishing Co. Pvt. Ltd. 2010
[12]. Sood Vivek, Cyber Crimes, Electronic Evidence and Investigation: Legal Issues, Nabhi Publication, 2010
[13]. Harish Chander "Cyber Laws and IT Protection" published by PHI Learning Private Limited New Delhi,2012
[14]. Haq S and Khan B.L." E-Banking Challenges and opportunities in The Indian Banking Sector" published in Innovative Journal of Business and Management 2: 4 July – August (2013) available at www.innovativejournal.in
[15]. Uppal R.K."Internet banking in India: Emerging Risks and New Dimensions" published in Prime Journal, Business Administration and Management (BAM) Vol. 1(3), March 10th, 2011 visit www.primejournal.org/bam
[16]. Hota J."Growth of ATM Industry in India" published in CSI Communications February 2013
[17]. Behra A. "Cyber Crime and Law in India", Indian Journal of Criminology and Criminalistics, 2010; p. 16-30. available on http://www.nicfs.nic.in/janjune2010.
[18]. cyber extortion risk report 2015, NYA International, Oct 2015
[19]. CRIC. (2005). Trojan redirector ups the ante in online banking attacks, cyber criminal investigation cell. Crime Branch Criminal Investigation Department Mumbai India
[20]. "Home - JPMorgan Chase & Co"
[21]. PandaLabs. (2012). The Quarter at a Glance, Quarterly Report. Retrieved from the website:http://press.pandasecurity.com/wp-content/uploads/2012/08/Quarterly-Report-PandaLabs-April-June-2012.pdf
[22]. Kharouni, L. (2012). Automating online banking fraud, automatic transfer system, the latest cybercrime toolkit feature, trend micro incorporated research paper. Retrieved from the website: http://www.trendmicro.com.br/cloud-content/us/pdfs/security-intelligence/white-papers/wp_automating_online_banking_fraud.pdf
[23]. DOPUK. (2013). Bank-distributed denial of service (DDoS) attacks strikes could presage Armageddon. DoS Protection UK. Retrieved from the website: http://www.dos-protection.co.uk/?p=152
[24]. Unknown. (2006). Denial of Service / Distributed Denial of Service MANAGING DoS ATTACKS, Trusted Information Sharing Network for Critical Infrastructure Protection, Commonwealth of Australia
[25]. John La Cour (April 29, 2014) vishing campaign steals a card from customers of dozens of banks [online] Available at www.blog.phishlabs.com
[26]. Umashankar sivasubramannian vs ICICI bank 2008, Tamil Nadu
[27]. Kumar, D (2005) "phishing for trouble Jan 20, 2007
[28]. Article on one of the three cyber attacks in banks successful by Riju Mehta April 27, 2017, economic times.
[29]. manager axis bank ltd vs sai Sandeep Bhosle AIR 2017
[30]. https://www.indiatoday.in/india/story/hackers-steal-rs-94-crore-from-pune-s-cosmos-bank-1314081-2018-08-14
[31]. https://www.business-standard.com/article/companies/amazon-hit-by-extensive-fraud-hackers-stole-money-from-100-seller-accounts-119050900110_1.html
[32]. https://www.forbes.com/sites/jeanbaptiste/2019/08/15/hackers-stole-over-4-billion-from-crypto-crimes-in-2019-so-far-up-from-1-7-billion-in-all-of-2018/#4362b64355f5
[33]. https://www.indiatoday.in/india/story/punjab-mp-preneet-kaur-rs-23-lakh-fraud-jharkhand-cybercrime-1578507-2019-08-08
[34]. https://thehackernews.com/2019/01/ukrainian-cybercriminals.html
[35]. https://thehackernews.com/2019/01/magecart-hacking-credit-cards.html
[36]. https://thehackernews.com/2018/11/nodejs-event-stream-module.html
[37]. https://techcrunch.com/2018/09/19/newegg-credit-card-data-breach/
[38]. https://thehackernews.com/2018/10/bank-atm-hacking.html
[39]. Strategic national measures to combat cyber-crime: Perspective and learnings for India, available at: http://www.ey.com/Publication/vwLUAssets/ey-strategic-national-measures-to-combat-cybercrime/$FILE/eystrategic-national-measures-to-combat-cybercrime.pdf
[40]. Reserve Bank of India, Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, (21 Jan 2011).
[41]. Gordon, Sarah. "On the definition and classification of cybercrime"(PDF)
[42]. Laqueur, Walter; C., Smith; Spector, Michael (2002). Cyberterrorism. Facts on File. pp. 52–53
[43]. Section 3(2), Information Technology Act, 2000 provides authentication of Electronic Records shall be effected by the use of an asymmetric crypto system and hash function which envelopes and transform the initial electronic record into another electronic record.
[44]. RBI for two-stage verification for online banking transactions, Economic Times, Mumbai, April 22, 2014
[45]. RBI Guidelines on Information Security, Electronic Banking, Technology Risk management, and Cyber Frauds, 2012.
[46]. Role of RBI in the Indian banking system, available at https://www.quora.com
[47]. RBI's new guidelines to customers against online fraud written by Deepika uploaded in 2017 available at https://www.oneindia.com