National Journal of Advanced Research
ISSN: 2455-216X; Impact Factor: RJIF 5.12
Received: 05-08-2019; Accepted: 08-09-2019
www.allnationaljournal.com
Volume 5; Issue 4; October 2019; Page No. 53-58

Cyber security attacks in banking sector: Emerging security challenges and threats

Dr. S Krishnan
Assistant Professor, Seedling School of Law and Governance, Jaipur National University, Jaipur, Rajasthan, India

Abstract
Financial cybercrime in India has been steadily increasing over the years. For the year 2015-16, the Reserve Bank of India (RBI) reported 16,468 cybercrimes related to ATM, debit card, credit card and net banking frauds. Financial sector faced almost three times the cyber-attacks as compared to that of the other industries. This paper seeks to provide a view of the current cyber threats targeting the banking industry in order to promote dialogue on collective protection strategies. The cyber challenge will remain complex. Threats will evolve rapidly with the development of new technologies, the ever changing geo-political landscape and, not surprisingly, from our efforts to counter them.

Keywords: Cyber threats, cyber security, cross site scripting, Block chain

1. Introduction

Cyber threats are attempts to infiltrate or disrupt a computer network/system. These threats may originate from a variety of sources and any website or computer can be a potential target. Cyber threats may also target individuals or businesses in an attempt to obtain sensitive information through online channels.A cyber threat is any malicious act that attempts to gain access to a computer network without authorization or permission from the owners. There is no disputing that cybercrime is at an all-time high. It seems not a day goes by without an organization suffering a security breach or customers of a major bank having money stolen from their accounts. One of the main targets for cybercrime is without a doubt banks. In the last year, banks from all over the world have been hit by hackers. So why are banks such a gainful target for cybercrime? The answer is simple, cyber criminals go where the money is, and banks have more money than other organizations. Recently "Wannacry" ransonmare created huge ruckus around world is a frightening reminder of the vulnerability of a connected world.

Cybersecurity is a growing risk area for all businesses at the moment. In particular, over the past year it has become glaringly obvious that there are a number of gaps in cybersecurity protection and infrastructure when it comes to the banking sector. As financial institutions shift to digital channels like online banking and mobile banking, the attack surface grows, and there is more to protect. The threat of cybercrime on the global banking and financial industry is apparent with a tectonic increase in cases over the past few years. These attacks have become highly targeted from hacking the bank accounts of individuals, companies, governments and demanding heavy ransoms to decrypt the data that was force-encrypted.

2. **Cyber security in Banks**

A bank runs multiple servers that store enormous amount of information and details of various operations such as credit cards, ATMs, real time gross settlements, ATMs and SWIFT (the global financial messaging service banks use to move funds), among others. Over the past few years, banks have been fighting cyber-attacks like 'distributed denial of service' (or DDoS), considered the most common type of cyber-attack on financial institutions, worldwide.

Cybersecurity attacks are increased in the banking industry during 2016, and they have not shown any signs of abating. The risks are prevalent across all areas of the sector—with banks both large and small suffering losses from cybersecurity breaches. Now a days banks are increasing amount of banking transaction through online. Banks can offer increased access and convenience to customers because of this digitization; however, this has also opened the door to increased online security risks—from numerous types of attackers that can include

insiders, various levels of thieves, people with political agendas and other third parties. Customers and stakeholders are left wondering, how will banks address the gaps in cybersecurity?

Understandably, at numerous banks and financial institutions, chief risk officers have identified cyber-threats as their top priority for 2017. This issue has been moved to the forefront of bank-board meeting agendas, and senior managers must act fast to diminish these growing threats to banks. Technological skill and access to resources for attackers have been growing at a faster pace than the defence-mechanism efforts have been enacted by banks. This needs to be tackled head-on in 2017 in order to get ahead of the problem.

Cyber-attacks can take on many forms—most commonly the attackers are seeking to acquire capital as well as confidential data and sensitive information. Based on the number of recent attacks, it is fair to estimate that many banks are unprepared to deal with major cybersecurity attacks and need to address their financial-crime security efforts across the board. 2017 will be a first and foremost year for assessing the extent of the gaps in cybersecurity. Before being able to devise a strategy or solution to close these gaps, banks need to tackle the challenge of identifying the gaps themselves—they must apply an intelligence-based approach in order to devise a comprehensive strategy. This in itself will be a significant task that will require the application of cybersecurity-skilled specialists.

3. Cyber Security Framework for Banks

In October 2016, the Reserve Bank of India directed banks to implement a security policy containing detailing their strategy to for dealing with cyber threats and including tangible "cyber-hygiene" measures. This was following a renewed emphasis on the early implementation of the RBI's Cyber Security Framework in banks. The RBI had first notified the 'Cyber Security Framework' in Banks in June 2016. The Framework was a successor to broad guidelines on information security and cyber frauds which had been issued in line with the recommendations of the Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds in 2011.

As per data reported by the Reserve Bank of India (RBI), the number of cybercrime pertaining to credit card, ATM, debit card and Internet banking shows a marginal increase of 4.4% from 13,083 in 2014-15, to 13,653 in 2016-17.

RBI has issued instructions to banks for reversal of erroneous debits arising from fraudulent or other transactions, and for Board-approved bank policy to cover customer protection, the mechanism of compensating the customer for the unauthorised electronic banking transactions, and display of the same on the bank's website, along with the details of grievance-handling / escalation procedure. Under the Banking Ombudsman Scheme, if a customer does not receive any reply within a period of one month after receipt of representation by the bank or is not satisfied with the reply given, he can file a complaint before the Ombudsman, who can ask the bank to pay compensation of up to Rs. 20 lakh to the customer for loss, suffered by the customer due to an act of omission of the bank, and also compensation of up to Rs. 1 lakh for mental agony and harassment.

The Framework is geared towards minimising data breaches and implementing immediate containment measures in the event of such breaches. It emphasises the urgent need to put in place a robust cyber security and liveliness framework and to ensure continuous cybersecurity preparedness among banks. The Framework also mandates the adoption by banks of a distinct cybersecurity policy to combat threats in accordance with complexity of business and acceptable levels of risk within a set deadline. Further, the framework requires the earliest setting up ofSecurity Operations Centres within banks for continuous investigation, disallowing un-authorised access to networks and databases, protection of customer information and the evolution of a cyber crisis management plan.Blockchain model is suggested to the financial institutions to secure their business transactions.

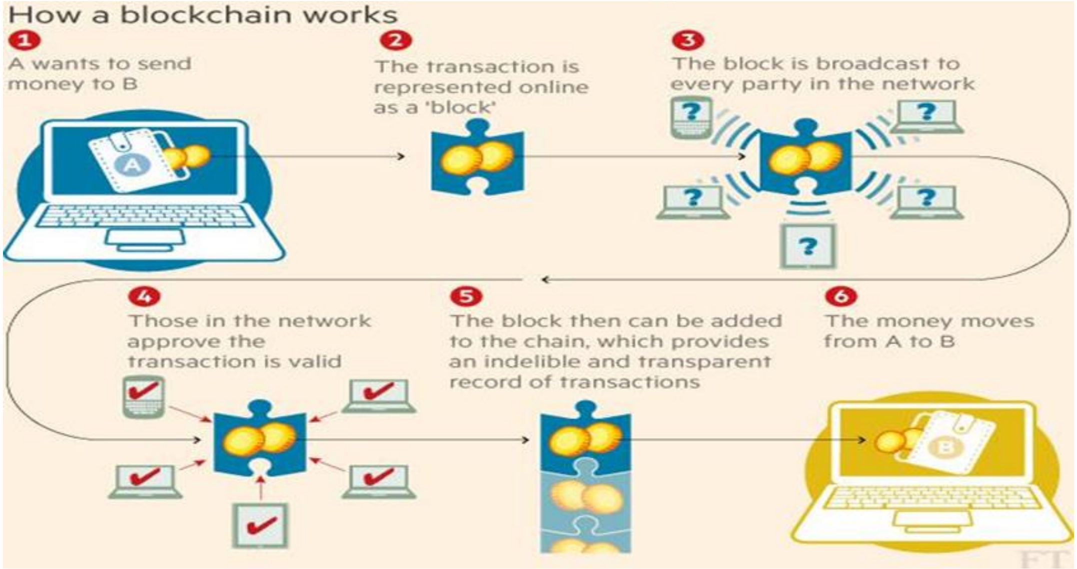
How a blockchain works
1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
A
B
FT

Fig 1

4. Steps to be taken to secure from cyber threats

Thereis urgent need to update the policy framework and make concerted and committedefforts to develop robust cyber security systems in our country. Fortunately, Indian government has set up a Cyber Swachta Kendra – Botnet cleaning and malware analysis centre, which is providing tolls like USB Pratirodh, SamvidApp, M-Kavach etc.,

Centralgovernment must enhance cyber hygiene among all end-users and to create asecure and safe internet ecosystems and The Centre Emergency Response Team(CERT-In) must co-ordinate required tasks.

Banks must practice a rigid cyber hygieneregimen to prevent malware infections on their systems and to ensure securitythrough suitable anti-malware.

The other area that requires immediate attention is to increase insurance coveragefor cyber-attacks. With rise in malware attacks, banks face increasing risks incyber space. Such attacks may lead to operational and other securityinterruptions.

Bankshas to aware their customers about cyber attacks and measures to be taken to staysecure and not to breach any sensitive data.

Banks must also have an eye on insiders as there are instances where the employeesleaked highly secured data for their malicious desires.

To proactively manage the vulnerabilities that could be exploited by hackers, updates have been rolled out by SWIFT, banks must follow them.

Additionally, the Reserve Bank of India (RBI) as released a set of guidelines to manage the risks associated with suchattacks. RBI's circular last year covered several notable suggestions, ranging from arrangements for continuous surveillance, creation of a cyber security policy etc., RBI also constituted Meena Hemachandra Committee to frame recommendations on Information Technology and Cyber Security.

Compared to today, the secure bank of the future will use more machine-learning technology and systems to proactively prevent potential breaches and data loss.

So, banks must ensure proactive prevention, and more unique layers of defence to protect the banks value at most.

So it is more than obvious now that the cyber vulnerabilities have massive global implications, so banks needs to push for global rules on such issues otherwise our banks will be on tenterhooks whenever ransomware – like cyberattacks take place.

5. Review of literature

Claessens et al., (2002) there are number of frauds or cybercrimes witnessed in the banking sector, like ATM frauds, Cyber Money Laundering and redit 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 some other bank account. 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.

Moore.T, Clayton.R&Anderson.R (2009) focused on the subject of online crime. Online crimes mostly occur from the nuisance came from amateur hackers. This paper looks at the data of online crime and many problems. Problems that banks and police forces face in controlling the traditional law enforcement. The analysis of this paper show that significant improvements are possible in the way dealing with online fraud and to study the online crime it is suggested that to understand its economic perspective.

Florêncio&Herley, (2011) 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 combat such crimes.

6. Security Considerations

While each bank thinks distinctively on adopting various considerations it is imperative to assume that the theme remains the same for various banking channels:

Internet Banking: Security controls like multi factor authentication, creation of strong passwords, adaptive authentication, image authentication, etc. can be considered.

Mobile Banking: It should be ensured that mobile applications are up to date and should be tested. Latest hardening standards could be implemented.

Wallet Transactions: Awareness material on Phishing, Malware attacks, vishing and social engineering, Password security etc. should be incorporated.

ATM Security: Biometrics like eye-retina, voice scan or fingerprint scan should be introduced by banks.

Some of the Cyber Security Attacks on Banks

Banks are exposed to a number of cyber security attacks. RBI in [1] identifies Phishing, Cross site scripting, Vishing, Cyber-Squatting, Bot networks, E-mail related crimes, Malware, SMS spoofing, Denial of service attacks, Pharming, Insider threats as the emerging information security attacks on banks.

Phishing

One of the most common cyber frauds is ―Phishing‖. Phishing is an attack in which an attempt is made to obtain sensitive information of user such as usernames, passwords, credit card details, etc. by an attacker by pretending to be a reliable body in an electronic communication. Phishing is typically carried out by email spoofing or instant messaging in which users are asked to click on a link usually for securing their accounts. The users are then directed to fraudulent websites which look alike the original banking website so that the user is deceived and is asked to enter his personal information such as usernames, passwords, credit card details, etc. Once the user enters his/her personal information, the fraudster then has access to the customer's online bank account and to the funds contained in that account. There are a variety of tools and techniques used by phishers which serve a variety of functions, including email delivery, phishing site hosting, and specialized malware. These tools include Botnets, Phishing Kits, Abuse of Domain Name Service (DNS), Technical Deceit, Session Hijacking and Specialized Malware [19].

A phishing incident was reported in Hyderabad [20], which was in the name of India’s central bank RBI in which the phishing email said that RBI had launched a new security system and asked users to click a link which redirected users to a fake website. It asked users to enter their online bank credentials including card numbers and the secret three digit CVV number, among others. RBI has cautioned people that it has not launched any such software as soon as it came to know about it.

Cross site scripting

Cross-site scripting (XSS) is a kind of cyber security vulnerability usually found in web applications and they allow code injections by malicious web users into the web pages that are viewed by other users. Examples of such code include client-side scripts, HTML code, etc. A cross-site scripting vulnerability can be exploited by attackers to bypass access controls. Their impact ranges from a petty nuisance to a significant security risk, depending on the sensitivity of the data that is handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner.

Vishing

Vishing is a cyber-attack in which social engineering and Voice over IP (VoIP) are used to access the private and financial information from the public for getting financial reward [1]. It combines "voice" and ―phishing‖. Vishing is an illegal practice where an attacker calls a user and pretends to be from a bank in which the user has an account. He usually asks to verify the user’s account information (stating that user’s account has been suspended, etc.) and once the user gives his credentials such as username, password, credit card number, etc., the attacker has easy access to the user’s account and the money in it. There has also been a theft of payment card data of the customers of U.S. banks by various vishing attacks. In an attack in 2014, customers of a midsize bank received SMS text messages which claimed their debit card was deactivated and asked users to provide the card and PIN numbers to reactivate it [21].

Cyber squatting

Cyber-squatting is a process in which a famous domain name is registered and then it is sold for a fortune. Cyber Squatters register domain names which are similar to popular service providers' domains so as to attract their users and benefit from it. Some countries have specific laws against cyber-squatting that are beyond the normal rules of trademark law. For example, the United States has the U.S. Anti-cybersquatting Consumer Protection Act (ACPA) of 1999 which provides protection against cybersquatting for individuals and also owners of distinctive trademarked names. The Washington Post reported in 2007 that Dell filed a lawsuit against BelgiumDomains, CapitolDomains, and DomainDoorman for cyber-squatting and typo-squatting and dellfinacncialservices.com was one of the domains that was cited [22].

Bot Networks

Bots are programs that infect a system to provide remote command and control access via a variety of protocols, such as HTTP, instant messaging, and peer-to-peer protocols. Several of bots under common control are commonly referred to as a ―Botnet‖. Computers get associated with botnets when unaware users download malware such as a ―Trojan Horse‖ which is sent as an e-mail attachment. The systems that are infected are termed as ―zombies‖. Illicit activities can be carried out with bots by the controller that include relays for sending spam and phishing emails, updates for existing malware, DDOS ,etc. Bot Networks create unique problems for organizations because they can be upgraded very quickly remotely with new exploits, and this could help attackers prevent security efforts.

Malware

Malware is a maliciously crafted software program that accesses and alters the computer system without the consent of the user or owner. Malware includes viruses, Trojan horses, worms, etc. Malware can heavily influence the confidentiality, integrity and availability of the banking system. Malwares have the capability to compromise the information in the banking systems and may lead to a loss of worth millions to the bank. Malwares can target both the user's system and the bank itself. E.g; Zeus.

Denial of Service (DOS) Attack

A DOS is an attack in which a user or an organisation is prevented from accessing a resource online. While as in Distributed denial-of-service Attack (DDOS), a specific system is targeted by a large group of compromised systems (usually called a Botnet) and make the services of the targeted system unavailable to its users.Actually the targeted system is flooded with incoming messages which causes it to shut down and thus the system is unavailable to its users.

Although DOS attacks don't usually result in loss of information or security to a bank, it can cost the bank a great deal of time, money and customers and can also destroy programming and files in affected computer systems.

SMS Tricking

It is a relatively new technology in which a user receives a SMS message on phone which appears to be coming from a legitimate bank. In this SMS the originating mobile number (Sender ID) is replaced by alphanumeric text. Here a user may be fooled to give his/her online credentials and his/her money may be at risk of theft.

TCP/IP Spoofing

It is one of the most common forms of online camouflage. In IP spoofing, illegal access is attempted on a system by sending an email message to a victim that appears to come from a trusted machine by ―spoofing‖ the machines' IP address. IP address spoofing is a powerful technique as it can enable an attacker to send packets to a network without being blocked by a firewall. This is because usually firewalls filter packets based on sender's IP address and they would normally filter out any external IP address. However using IP spoofing, the attacker's data packet appears to come from legitimate IP address (internal network) and thus firewall is unable to intercept it. The main goal here is to obtain root access to the victim's server (here the banking system), allowing a backdoor entry path into the targeted systems [5].

Pharming

It is also called farming or DNS poisoning. In this attack whenever a user tries to access a website, he/ she will be redirected to a fake site. Pharming can be done in two possible ways: one is by changing host's files on a victim's computer and other way is by exploiting vulnerability in DNS server software. In January 2005, the domain name for a large New York ISP, Panix, was hijacked and legitimate traffic was redirected to a fake website in Australia [23] No financial losses are known. In January 2008, a drive-by pharming incident was reported by Symantec that was directed against a Mexican bank and in which the DNS settings on a customer's home router were altered after receipt of an e-mail message that appeared to be from a legitimate Spanish-language greeting-card company.

Insider Threats

With the increase in the use of information technology by banks, there is a high security risk to bank's data by insiders or employees of banks who can disclose, modify or access the information illegally. Also unintentional errors by employees can have devastating results. Healthy security processes must be used by banks to lessen such threats.

OTP Attacks

OTP(one Time Password) is a two factor authentication method in which a password is created whenever the users attempts authentication and the password is disposed of after use. A no. of attacks can be launched on accounts that are OTP protected which are known as MIT-X methods (Man-In –The-X) [9]. These are as follows:

Man-in –the-middle attack (MITM): Here the transmission paths of data are accessed and information is snatched in the middle of transactions.

Man-in-the-Browser attack (MITB): Here malicious code exists in the web browser and it induces users to enter credentials and other important information into a fake form.

Man-in-the-PC attack (MITPC): MITPC exploits the weaknesses in the hardware environment or operating system to steal OTP.

Security Challenges

The rapid growth of digital payments platform in India and the impetus towards a cashless economy has renewed focus on the need to strengthen cybersecurity posture. The following are the some of the Challenges.

Strict compliance regulations: Managing regulatory compliances has become enormously challenging for the banks. Over the past few years the volume of regulations has increased dramatically. Along with the larger banks, smaller ones too are required to fulfil the regulatory obligations

The struggle to secure customer data: There are number of ways in which violation of privacy can take place in banking sector like stolen or loss card data, unauthorized sharing of data with third parties and loss of client's personal data due to improper security measures

Third party risk: Banks need to conduct due diligence on third parties they are associated with. As per Payments card industry data security standard, third parties need to report any critical issues associated the card data environment to the bank.

Evolving cyber threat landscape: The development in technologies is leading to the latest cyber threats like next generation ransomwares, web attacks etc.

Transaction frauds: Fraud detection technologies should be in place with proper consideration of risks based on the business factors.

Secure SDLC: Banks need to incorporate SDLC security for banking products and applications.

7. Recommendation to Prevent Cyber Crime

1. Cyber Fraud Council in Banks

Whenever a cyber-fraud is committed the victim should report to the Cyber Fraud Council that must be set up by in each and every bank to review, monitor investigate and report about cyber-crime. In case, such Council does not take perform or refuses to perform its duty then a provision to file an FIR must be made. The matter to be brought before such council can be of any value. However, when the value is high then the Council shall act expeditiously. RBI in its 2011 Report stated that when bank frauds are of less than one Crore then it may not be necessary to call for the attention of the Special Committee Board

2. Education to Customer

The customer should be educated and made aware about various bank frauds and measures should be informed to them for safety mechanisms so that they do not fall prey as victims of cyber- crime. If a customer is conscious and report the matter of cyber-crime then in the initial stage also instances of cyber-crimes can be reduced. A customer should be made aware about the Dos and Don'ts' of E-banking. It can be done through publishing it on the bank's website, publishing in the newspaper, through advertisements, by sending SMS alerts, through poster education etc. In case a bank introduce any new policy or there are any changes which are required to be followed by all banks as per RBI then, bank must inform the customer through mails or by informing the customer through telephone. The awareness material should be timely updated keeping in mind the changes in the legislation and guidelines of RBI

3 Training of Bank Employees

Training and Orientation programs must be conducted for the employees by the banks. The employees must be made aware about fraud prevention measures. It can be done through newsletters or magazines throwing light on frauds related aspects of banks by senior functionaries, putting up 'Dos and Don'ts' in the workplace of the employees, safety tips being flashed on screen at the time of logging into Core Banking solution software, holding discussions on factors causing cybercrime and actions required to be undertaken in handling them. Employees who go beyond their call of duty to prevent cyber frauds if rewarded will also enhance the work dedication

4. Strong Encryption-Decryption Methods

E-banking activities must be dealt using Secure Sockets Layer (SSL). It provides encryption link of data between a web server and an internet browser. The link makes sure that the data remains confidential and secure. As per India, we follow asymmetric crypto system which requires two keys, public and private, for encryption and decryption of data.For SSL connection a SSL Certificate is required which is granted by the appropriate authority under IT Act, 2000. To ensure security transactions RBI suggested for Public Key Infrastructure in Payment Systems such as RTGS, NEFT, Cheque Truncation System. According to RBI it would ensure a secure, safe an sound system of payment. Wireless security solutions should also be incorporated. In cases of Denial of Service Attacks, banks should install and configure network security devices.

5. Data protected technology adoption

Block chain is a technology that was initially developed for Bitcoin, the cryptocurrency. Block chain could reduce banks infrastructure costs by US$ 15-20 billion per annum by 2022. Block chain have the potential to transform how the business and the government work in vast variety of contexts.

8. Conclusion

Information Technology has become the backbone of the banking system. It provides a tremendous support to the ever increasing challenges and banking requirements. Presently, banks cannot think of introducing financial product without the presence of Information Technology. However Information Technology has an adverse impact too on our banking sector where crimes like, phishing, hacking, forgery, cheating etc. are committed. There is a necessity to prevent cyber-crime by ensuring authentication, identification and verification techniques when a person enters into any kind of banking transaction in electronic medium. The growth in cyber-crime and complexity of its investigation procedure requires appropriate measures to be adopted. According to National Crime Records Bureau it was found that there has been a huge increase in the number of cyber-crimes in India in past three years. Indian banking sector has carried out all their banking activities through electronic medium as the study suggest that there has been an increase in the number of payments in online banking. However, the change in the banking industry must be such which suits the Indian market. The only propitious step is 'to create awareness among people about their rights and duties and to further making the implementation of the laws more firm and stringent to check crime'.

9. References

1. Changsok Yoo, Byung-Tak Kang, Huy Kang Kim. Case study of the vulnerability of OTP implemented in internet banking systems of South Korea‖, Multimed Tools Appl. 2015; 74:3289–3303.
2. Claessens J, Dem V, De Cock D, Preneel B, Vandewalle J. On the security of today s online electronic banking systems. Computers & Security. 2002; 213:253-265.
3. Ellen Messmer. ―First case of drive-by pharming identified in the wild‖ [Online], 2008, Available: http://www.networkworld.com/article/2282527/lan-wan/first-case-of--drive-by pharming--identified-in-the-wild.html
4. Florêncio D, Herley C. Where Do All The Attacks Go? Economics of Information Security and Privacy III pp.. Springer New York, 2011, 13-33.
5. Gopalakrishna G. Report of the Working Group on information security, electronic banking, technology risk management, and tackling cyber frauds‖, RBI, Mumbai, Maharashtra, 2011.
6. Jason Milletary. Technical Trends in Phishing Attacks‖, US-CERT
7. John La Cour. Vishing campaign steals card data from customers of dozens of banks [Online], 2014, Available: http://blog.phishlabs.com/vishing-campaign-steals-card-data-from-customers-of-dozens-of-banks
8. MohdKhairul Ahmad, Rayvieana Vera Rosalim, Leau YU Beng and Tan Soo Fun. Security issues on Banking Systems‖, International Journal of Computer Science and Information Technologies. 2010; 1(4):268-272.
9. Moore T, Clayton R, Anderson R. The Economics of Online Crime" , Journal of Economic Perspectives, Volume 23, Issue no.3, Summer 2009, 3-20.
10. Pharming‖, Wikipedia Available: https://en.wikipedia.org / wiki/Pharming#cite_note-3
11. Kaur RP. Statistics Of Cyber Crime In India: An Overview‖, International Journal of Engineering and Computer Science. 2013; 2(8):2555-2559,
12. Special Advisory –Data Breach in Indian Banks, 2016 www.mitkatadvisory.com
13. Top Ten Cyber Squatter Cases Available: http://www.computerweekly.com/photostory /2240107807/Photos-Top-ten-cybersquatter-cases/1/ Cybersquatting-cases-Number-10-Dell