Emerging Information Technology in Indian Banking Sector and its Cyber Security

Sivathas P
Assistant Professor, Government Law College
Dharmapuri, Tamilnadu, India

Abstract

Our world is changing fast and with it, so is the information technology that drives it. Collaboration and hybridization are quickly becoming the new normal, through the smart use of innovative technologies and new delivery models. This is happening in all fields because of the immortal desire to make things simpler. The use of Personal Computer (PC) banking or online banking or internet banking or e- banking saved us from many hours and simplified live in many ways. The quick and speedy availability of access to internet expands every walks of life of human being. The facility to transact money without the physical and personal appearance before the bank counters' ease the customers to do lot in trade and commerce. In this digital world, the data are communicated through electronic means and the question is whether it is securely transmitted and protected? At many times, the answer is "not known" or "no". When internet banking was introduced in the country, it was felt that having a password-protected account was adequate to ensure safety, but not anymore. The cyber threat landscape has changed. A few years ago, most frauds were related to identity thefts, the techniques adopted by fraudsters were easy to trace and these did not involve big money either. But over the years, online heist has become an organized crime. Hackers are spread across the globe. The attacks involve compromising a bank's database with system level implications. Hence, this article discusses the type of threats and measures to sustain or combat the cyber insecurity and also the legal framework available in India.

Keywords: *Internet banking, E-banking, Legal issues, cyber security.*

I. INTRODUCTION

The use of internet access has simplified our lives in many ways. Just imagine how many hours we have saved because we can book tickets online or conduct banking transactions via the internet. Internet banking sometimes called online banking is an outgrowth of Personal Computer (PC) banking. Internet banking uses the Internet as the delivery channel by which to conduct banking activity, for example, transferring funds, paying bills, viewing and checking savings account balances, paying mortgages, purchasing financial instruments and certificates of deposit. Internet banks are also known as virtual, cyber, net, interactive, or web banks.

II. THE INTERNET OF THINGS

The Internet of Things (IOT) is an expanding and heterogeneous universe encompassing all things which are capable of connectivity and are equipped with sensing and actuating capabilities. The presence of things in our everyday life gives to many problems, viz; Surveillance, commercial exploitation of big data and security. Cookies, web beacons, device fingerprinting and kindred phenomena are Internet of Things, but it is submitted that cross-device tracking is what is more directly relevant to the IOT and may be more dangerous since people are not aware of it[1].

III. NET NEUTRALITY

Net neutrality is a hot topic. One should welcome the ruling of the Telecom Regulatory Authority of India (TRAI), which reaffirms the principle of net neutrality[2], whereby, moving from the assumption that everybody has a fundamental right to access the Internet, this access and the relevant use must be granted in a non-discriminatory way. A poll conducted by the BBC found that four in five adults consider the right to internet as a fundamental human right.

IV. ELECTRONIC BANKING

It is an umbrella term for the process by which a customer may perform banking transactions electronically without visiting a brick-and-mortar institution. The following terms all refer to one form or another of electronic banking: PC banking, Internet banking, virtual banking, online banking, home banking, remote electronic banking, mobile banking and phone-banking. PC banking and Internet / online banking are the most frequently used designations. It should be noted, however, that the terms used to describe the various types of electronic banking are often used interchangeably. PC banking is a form of online banking that enables customers to execute

[1] Guido Noto La Diega, "The Internet of Citizens: A lawyer's view on some technological developments in the United Kingdom and India", 12 IJLT 53 (2016), SCC Online Web Edition accessed on Dec 27, 2017.

[2] TRAI regulations, no. 2/2016 of February 8, 2016, Prohibition of discriminatory tariffs for data services regulations (2016) available at http://www.trai.gov.in/WriteReadData/WhatsNew/Documents/Regulation_Data_Service.pdf.

bank transactions from a PC via a modem or Wi-Fi. Currently, many banks offer PC banking systems that allow customers to obtain account balances and credit card statements, pay bills and transfer funds between accounts.

E-banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels[3]. Customers access e-banking services using an intelligent electronic device, such as a Personal Computer (PC), Personal Digital Assistant (PDA), Automated Teller Machine (ATM), Kiosk, and smart phone.

V. CLOUD COMPUTING

Cloud computing is a cost effective method to share computing resources of a large scale that can be accessed from any part of the world. Any individual user or company that has the permission to access the cloud infrastructure can use its processing power to run an application, store data, or perform any other computing task. Cloud computing service providers in India are Internet intermediary within the meaning of Information Technology Act 2000 (IT Act 2000) and they are also required to comply with the cyber law due diligence requirements[4]. Cloud computing is a commercial project, that most of the IT vendors of the world love to launch in India. This is so because India has a large market for cloud computing business. Netmagic (2013-14), NTT Communications Company is a subsidiary of Nippon Telegraph and Telephone Corporation of Japan[5] (NTT) was the first in India to launch services like cloud computing and managed hosting service provider.

VI. ANDROID APPLICATIONS ON BANK TRANSACTIONS.

Now-a-days many mobile phone applications (mobile wallets) are coming into the market through service providers, to do banking transactions, bill payment, recharge of prepaid mobile and e-commerce activities. The android applications can be classified into bank applications and Virtual e-wallet or Virtual Money bank. Some of the applications are (a) Axis Bank Lime, (b) HDFC bank PayZapp, (c) ICICI Pockets, (d) SBI Buddy, (e)State Bank Anywhere Personal, (f) SIB Mirror, (g) BHIM App, (h) Jio Money, (i) Mobikwik, (j) mRupee, (k) Paytm, (l) Airtel Money, (m) Vodafone M-pesa and (n) IndPay etc.,

VII. CYBER INSECURITY

India is ranked third globally in terms of vulnerability, accounting for 6.5% of the total targeted attacks in 2012, according to California-based Symantec's Internet Security Threat Report, 2013.[6] Top emerging information security threats in the internet banking space are malware, social engineering and distributed-denial-of-service and phishing attacks.

Cyber security experts point out that the bigger problem in India is the secrecy, something that works in hackers' advantage. Most of the companies and banks who are hit by the hackers prefer to push it under the carpet. Now the Reserve Bank of India (RBI) has now made it mandatory for the banks to disclose the cyber attacks.

VIII. CYBER ATTACKS ON BANKS

While many banks in India, trust their cyber security strategy, nearly a third of all cyber attacks are successful, according to a report by Accenture. Even the bank executives are confident about their overall security strategy; the security attacks continue to remain a challenge for banks. A bank experienced 85 serious attempted cyber breaches each year, on an average, in addition to the phishing, malware and penetration attacks received each day. Of these attacks, about one third (36%) were successful, that is, at least some information was obtained through the breach. What was the sad news behind it was, it took 59% of the banks several months to detect the breaches.[7]

In July 2015, the Union Bank of India was breached by cyber hackers. The hackers had managed to get past the bank's security systems but the money trail was traced and the movement of funds was blocked.[8] In January 2017, hackers seized control of computers at three Indian banks and a pharmaceutical company and demanded to pay one bit coin per computer to unfreeze them. Later in investigations it was found that "Lechiffre ransomware" infection through email disguised as a communication from senior management was opened by some junior employees. The vulnerability of the banks came into light recently in the end of 2016, when data of about 3.2 million debit cards was lost. State Bank of India (SBI), HDFC bank, ICICI bank, YES bank and AXIS bank were worst hit by the breach of the debit cards[9].

IX. TYPES OF CYBER THREATS IN BANKING SECTOR

Different types of threats committed by hackers are as follows;

a) Computer viruses – a type of malicious software program, when executed alter or modify the normal working of computer.

b) Phishing – an attempt to obtain sensitive information like user id and password often

[3] http://slideplayer.com/slide/6918963/
[4] PTLB, "Cloud Computing Legal Issues in India", posted June 24, 2014 accessed on February 24, 2018.
[5] https://en.wikipedia.org/wiki/NTT Communications accessed on February 25, 2018.
[6] Gayathri Nayak, 'With internet banking on the rise, frauds are just a click away', Mumbai Ed., The Economic Times, 5th June, 2003, p.6.
[7] Riju Mehta, "One in three cyber attacks in banks are successful", Economic Times Bureau, April 27, 2017, 02.21 PM IST.
[8] Sachin Dave, "India witnessing sophisticated cyber attacks from organised and unorganised players", Economic Times Bureau, February 20, 2017, 12.41 PM IST.
[9] Ibid.

for malicious reason through electronic means.

c) Spoofing – a fraudulent practice in which communication is sent from an unknown source disguised as a source known to the receiver.

d) Phone phishing – voice phishing through phone call to access for financial reward.

e) Internet hacking – a malicious attacks on computer networks and its systems.

f) Fraudulent investment newsletter – fake newsletter or email letter

g) Credit card fraud – card data theft

h) Obfuscated spam – make spam emails to bypass filters.

i) Pharming – a scamming practice in which malicious code is installed in PC, misdirecting users to fraudulent websites.

j) Crimeware – a class of malware designed specifically to automate cybercrime.

k) SQL Injection – a code injection technique that might destroy your database.

l) Vishing Fraud: Fraudsters pretend themselves as bank officials, inform the customer regarding banking services in need and obtain card particulars, OTP information. Then one's money is swept away by online fraudulent transactions. This type of fraud is termed as Vishing Fraud. As per RBI guidelines, no bank will ask for bank or insurance related information from the customer through phone or e-mail.

m) Skimmer: a device secretly fixed to obtain swipe card information.

n) Lottery scam: Lottery scam is otherwise known as Nigerian Fraud / Advance Fee Fraud / 419 Fraud.

o) Loan scam: Ask the customer to advance money towards loan processing fee in unknown bank accounts through fake advertisements in newspapers and also through online.

X. COMBATING CYBER INSECURITY

A. *Ethical Hacking*

Many banks and companies including ecommerce and mobile app based service providers are increasingly roping in ethical hackers to look for loopholes in their system by continuously trying to hack into them from outside and report back to the company. Sometimes these ethical hackers also help companies fix the glitch. Security experts point out that the new age companies like Flipkart, Ola or Paytm are better prepared for the cyber hackers. These companies compared to the traditional companies have been proactive in tackling the threats[10].

B. *Choosing E-Banking Configuration*

E-banking systems rely on a number of common components or processes like Website design and hosting, Firewall configuration and management, Intrusion detection system or IDS (network and host-based), Network administration, Security management, Internet banking server, E-commerce applications (e.g., bill payment, lending, brokerage), Internal network servers, Core processing system, Programming support and Automated decision support systems. These components work together to deliver e-banking services. Each component represents a control point to consider. Through a combination of internal and outsourced solutions, management has many alternatives when determining the overall system configuration for the various components of an e-banking system.

C. *Reporting of Frauds*

With the advent of e-banking solutions, it also becomes necessary for the banks to adopt an increased level of security measures. In order to reduce, rather eliminate incidences of frauds and cyber frauds in the country, frauds should be immediately reported to Reserve Bank, in consonance with its classification and guidelines[11].

D. *Eliminating Multiple Authentication by the use of Biometric Technology*

Innovations like Biometric technology allows the person to be identified uniquely by evaluating one or more distinguishing biological traits like face, hand, retina, voice and ear features. The use of biometric authentication can eliminate the requirement of multiple passwords and PIN codes. The Indian banking sector is also gradually adopting biometric authentication to provide simple and secure banking experience to its customers[12].

E. *Precautions at ATM Booth*

a) Check for the skimmer tool at ATM Booth around card Reader Slot area.

b) Don't take help of outsiders at ATM Booth. Don't give ATM card to anyone.

c) Link your mobile phone with your bank account.

d) Don't allow outsiders at the time of withdrawal of money.

e) Keep a strict vigil on the movement of outsiders and cover your hand as you enter your PIN.

10 Supra 6.

11 Article by Varun Tripathi on "Frauds and Cyber Frauds in Banking Sector", SCC Online Web edition, accessed on Dec 27, 2017.

12 Dun & Bradstreet, "Emerging Technologies in digital banking in India", Forbes India, published on August 23, 2017 accessed on February 24, 2018.

F. Precautions at POS & Online Purchase of Goods:

a) At the time of purchase of goods or payment through card, use the swiping machine by yourself.

b) Cover the keypad with your free hand so that nobody can see what you type in.

c) Look for the skimmers, if any.

d) Precautions on Lottery Scam

e) When you receive any phone call or messages or e-mails regarding winning of lottery, then don't attract into those fake offers.

f) Never deposit any advance money in the unknown bank accounts.

g) Never give your personal information or banking credentials over phone or e-mail.

G. Precautions on Online Transactions:

a) Always login through genuine homepage or secured page (Website domain name starts with "https"). Https is used to protect highly confidential online transaction like online banking and online shopping order forms. Check for correct URL. Don't operate your online banking account if the website domain starts with http.

b) Never access your online banking account at Cyber cafes. Check for Key loggers at Cyber cafes. It is designed to secretly monitor and log all keystrokes.

c) Avoid clicking on links in messages, tweets, posts, and online advertising. These may be links to viruses or other forms of malicious content.

d) Disable location services when using apps.

e) Protect your computer by installing antivirus software or Anti-malware to safeguard.

f) Remember to log off when you're done.

g) Never access your online bank account or banking application in free Wi-Fi Zone.

h) Keep your mobile phones or tabs or laptops or PC applications secure through strong password / screen lock / pattern lock / PIN lock.

i) When bank or shop from your smart phone, log out of those sites once your transactions are complete.

j) Turn off Wi-Fi, Data connection and Bluetooth, when not in use.

H. Precautions to Use Mobile App for Banking Transactions

a) If you are new to payments via mobile apps, then you can mostly look at going either with mobile wallets or apps supporting UPI payments, depending upon your requirement.

b) UPI or Unified Payment Interface, is an electronic funds transfer instrument that enables all bank account holders to send and receive money from their smart phones without the need to enter bank account information or net banking user id/ password. This requires only the recipient's mobile number or Virtual Payment Address (VPA).

c) Most wallets also allow making payments by entering credit/debit card information, i.e. without first adding money. UPI is faster, if you are not comfortable storing your money in a 3rd party app.

XI. E-BANKING SERVICES AND THE RISK

Banking transactions can range from something as basic as a retail account balance inquiry to a large business-to-business funds transfer. E-banking services, like those delivered through other delivery channels, are typically classified based on the type of customer they support.

A. Weblink

A weblink is a word, phrase, or image on a webpage that contains coding that will transport the viewer to a different part of the website or a completely different website by just clicking the mouse. While weblinks are a convenient and accepted tool in website design, their use can present certain risks. Generally, the primary risk posed by weblinking is that viewers can become confused about whose website they are viewing and who is responsible for the information, products, and services available through that website.

B. Account Aggregation

Account aggregation is a service that gathers information from many websites, presents that information to the customer in a consolidated format, and, in some cases, may allow the customer to initiate activity on the aggregated accounts. Aggregation services can improve banking customer convenience by avoiding multiple log-ins and providing access to tools that help customers analyze and manage their various account portfolios. Once the customer's account is accessed, the aggregator copies the personal account information from the website for representation on the aggregator's site (i.e., "screen scraping"). Other aggregators use direct data-feed arrangements with website operators or other firms to obtain the customer's information. Generally, direct data feeds are thought to provide greater legal protection to the aggregator than does screen scraping.

C. Electronic Authentication

Verifying the identities of customers and authorizing e-banking activities are integral parts of e-banking financial services. The authentication methods

a) Passwords and personal identification numbers (PINs),

b) Digital certificates using a public key infrastructure (PKI),

c) Microchip-based devices such as smart cards or other types of tokens,

d) Database comparisons (e.g., fraud-screening applications), and

e) Biometric identifiers.

The authentication methods listed above vary in the level of security and reliability they provide and in the cost and complexity of their underlying infrastructures. As such, the choice of which technique(s) to use should be commensurate with the risks in the products and services for which they control access.

D. Website Hosting

Financial institutions that host a business customer's website usually store, or arrange for the storage of, the electronic files that make up the website. These files are stored on one or more servers that may be located on the hosting financial institution's premises. Website hosting services require strong skills in networking, security, and programming. Institutions developing websites should monitor the need to adopt new interoperability standards and protocols such as Extensible Mark-Up Language (XML) to facilitate data exchange among the diverse population of Internet users. Risk issues examiners should consider when reviewing website hosting services include damage to reputation, loss of customers, or potential liability resulting from (a) downtime,[13] (b) inaccurate website content, (c) unauthorized disclosure of confidential information and (d) damage to computer systems.

E. Payments for E-commerce and Bill Payments

Among the electronic payments mechanisms that financial institutions provide for e-commerce are automated clearing house (ACH) debits and credits through the Internet, electronic bill payment and presentment, electronic checks, e-mail money, and electronic credit card payments. Most financial institutions permit intra bank transfers between a customer's accounts as part of their basic transactional e-banking services. However, third-party transfers - with their heightened risk for fraud - often require additional security safeguards in the form of additional authentication and payment confirmation.

Financial institutions can offer bill payment as a stand-alone service or in combination with bill presentment. Bill presentment arrangements permit a business to submit a customer's bill in electronic form to the customer's financial institution. Customers can view their bills by clicking on links on their account's e-banking screen or menu. After viewing a bill, the customer can initiate bill payment instructions or elect to pay the bill through a different payment channel. The risk of potential liability for late payments due to service disruptions may arise.

13 i.e., times when website is not available.

XII. CONFERENCES ON E-SECURITY AND CYBER CRIME – A COMPARATIVE ANALYSIS

Internet banking is not limited to a physical site; some Internet banks exist without physical branches, for example, Telebank (Arlington, Virginia) and Banknet (UK). Initially, the awareness and discussion on online or internet security has started after the International De Droit Ponel Conference on “Computer Crime and Other Crimes against Information Technology” held in Wurrzburg, Germany (1992) organized by the Association Internationale Droit Ponel (ADIP)[14]. In this conference it is stated that only 5% of computer crimes were being reported to police. It continued with the European E-Commerce Directive 2000[15], where European community has adopted the Directive on Electronic Commerce containing set of rules which lay down the standards that will apply to various online intermediaries for their involvement in illegal or infringing material put on their internet facilities by third parties.

Then, In India, there was an International Conference on E-Security, Cyber Crime and Law in 2004[16]. One of the main issues for deliberation in the conference included was the electronic fund transfer and security of data banking and the need to improve the transmission standards and encryption methods. Cyber law, data protection and need for appropriate legislation for the purpose were highlighted by the delegates. The issues like policing the cyberspace, role of judiciary in digital age, network security and law were also extensively discussed in the conference.

XIII. SOFTWARE LAW AND CYBER LAW

Actually speaking, an Internet banking customer accesses his or her accounts from a browser or software that runs Internet banking programs resident on the bank's World Wide Web server, not on the user's PC. The Indian software law is based on the Indian Copyright Act 1957[17]. Though India is not a member of the Rome Convention of 1961, World Intellectual Property Organization (WIPO) Copyrights Treaty (WCT) and the WIPO

14 Draft Resolution of the ADIP Colloquium, October 5-8, 1992.

15 Directive 2000/31/EC of European Parliament and the Council on E-commerce dated June 8, 2000.

16 Held in Chandigarh, India on February 19th -20th 2004.

17 Extensively borrowed from the new Copyright Act of United Kingdom of 1956.

performances and Phonograms Treaty (WPPT), the Copyright Act is in compliance with it.

There is no specific law in India governing computer software like China. A computer software contract is governed by the common law principles as embodied in the Indian Contract Act 1872[18]. If the software is classified as "good", the Sale of Goods Act 1930 will have relevance in it. Section 2(7) of the said Act, is very wide and includes all types of movable properties, whether those properties are tangible or intangible. In Tata Consultancy Services case, the court held that the characteristics of (a) utility; (b) capable of being bought and sold; (c) capable of being transmitted, transferred, delivered, stored and possessed, satisfies for a "good", the same would fall under the section 2(7) of the Sale of Goods Act 1930[19].

Further, India is also the only country of the world where, phone tapping and e-surveillance is done without a Court Warrant (Judicial Warrant) and beyond the judicial scrutiny. The executive branch of Indian constitution is neither accountable to the parliament of India nor to the judiciary in this regard. All a police officer or authorized officer has to do is to approach the concerned cloud computing service provider, and it would hand over all your sensitive data and information to him without your knowledge. Further, even if the data is not physically handed over, access to the same can be given to such officer without anybody knowing of such access[20].

XIV. LEGAL ISSUES IN TECHNOLOGY BANKING IN INDIA

In India, We have no dedicated Internet banking laws but the Reserve Bank of India (RBI) has issued some guidelines in this regard. However, Internet banking risks in India are high and even RBI acknowledged risks of e-banking in India. Despite this position, banks in India are ignoring the cyber security due diligence requirements prescribed by RBI. The legal issues of Internet banking in India must be taken more seriously by all stakeholders especially the Indian banks. However, better results cannot be achieved till cyber security requirements made mandatory on the part of Indian banks[21].

To answer for the question, whether bank's negligence on online frauds or e-banking transactions will come under the purview of Consumer Protection Act, Hon'ble justice in para 10 and para 12 of the Judgment[22] stated that,

"The jurisdiction of the Consumer Fora exists to impart speedy and expeditious cheaper justice to protect the Consumers. Section 3 of the Consumer Protection Act, 1986 does provide efficacious, additional and supplementary remedy. Complaint cannot be thrown away merely because some complicated questions may arise. Consumer Fora do have ample powers to deal with the consumer disputes to solve them and protect the consumers".

A. Data Protection Law

There is no Data Protection Act in India unlike in Europe and UK[23]. The only provision which speaks about data protection is section 72 (Penalty for breach of confidentiality and privacy) section 72A[24] (Punishment for disclosure of information in breach of lawful contract) and section 43A[25] (Compensation for failure to protect data) of Information Technology Act 2000. It is a fundamental right of the individual to retain private information concerning him provided under Article 21 of the Indian constitution which says' "No person shall be deprived of his life or personal liberty except according to the procedure established by law".

B. Evidence and Cyber Law

Evidence is information that tends to prove or disprove a fact in question. Evidence may consist of documents, public records, affidavits or the testimony of witnesses. According to the United Nation Commission on International Trade law (UNCITRAL) on Electronic Commerce information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message[26].

The law of evidence is a part of the law of procedure. The Indian Evidence Act applies to all judicial proceedings before any court material. There are number of provisions applicable to electronic records etc., such as section 17, 18, 19, 20, 21, 22A, 32, 34, 35, 45, 46, 51, 57, 58, 60, 73,159 of The Indian Evidence Act 1872. The Indian parliament has amended the Act to effect the technology evidence before the court by inserting new section 22A (oral evidence as to contents of electronic records).

XV. CONCLUSION

Through rapid development of technology and Internet over the years, the question of cyber security has emerged as a global issue. The major issue is that the internet as a worldwide media can be accessed throughout the world and can be viewed in

[18] Thomas E. Soebbing, Article "A legal Comparison of the India software law and the software law of Germany; 10 IJLT (2014) 133, SCC online Web Edition accessed on Dec 27, 2017.
[19] Tata Consultancy Services Vs State of A.P. , (2005) 1 SCC 308 : (2004) 271 ITR 401.
[20] PTLB, "Legal framework for cloud computing in India", posted October 17, 2012 accessed on February 24,2018.
[21] Ramkkaushik, "Legal Issues of Internet banking in India", posted on Dec 25, 2012; PTLG Block; accessed on Dec 27, 2017.
[22] Supra 7.
[23] (2017) 7 GJLDP (April) 25, Article by Ranjit Singh, http://www.scconline.com, page 1 accessed on Dec 27, 2017.
[24] Inserted by the Information Technology (Amendment) Act, 2008 (10 of 2009) w.e.f. Oct 10, 2009.
[25] Ibid.,
[26] Article 7 UNCITRAL on Electronic Commerce.

any part of the world, so it is a disputable problem that which law will be applicable for such issue because of different cyber laws of countries. It becomes mandate for all the concerned banking sector organizations, governments and peoples to take coordinated action to prevent cyber insecurity. Cyber insecurity has become an international problem so it is the need of the hour to tackle it through a common legal strategy which has universal sanction.

From a customer perspective, awareness and education are the keys, which banks are taking seriously, as mandated by the RBI, through their websites, mails and sms to clients. Most frauds occur when customers show laxity in complying with security. Banks are also investing in adding more security features to customers' accounts. One of the features that banks added recently is the 'digitized signature'. Information for attack can also be gathered from a bank's staff. Awareness can act as a crucial fortress against cyber aggresses. The recent breaches have now led many banks to beef up their security systems. Some banks are now creating a parallel and a decoy IT system so that the hackers attack those instead of actual IT systems. We cannot say at anytime that there is cyber security in the digital world. But the cyber insecurity can be curtailed by proper program designing and remedied by an appropriate law when enacted or amended from time to time.

[1] http://perry4law.org/cyberlawsinindia/?p=119
[2] http://perry4law.org/blog/?p=118
[3] http://www.forbesindia.com/blog/digital-navigator/emerging-technologies-in-digital-banking-in-india/
[4] https://economictimes.indiatimes.com/industry/banking/finance/banking/one-in-three-cyber-attacks-in-banks-are-successful-report/articleshow/58396453.cms
[5] http://www.scconline.com
[6] http://slideplayer.com
[7] http://www.trai.gov.in