



International Journal of Engineering, Business and Enterprise Applications (IJEBA)

www.iasir.net

Comparitive Study of Online Banking Security System of various Banks in India

Rajpreet Kaur Jassal¹, Dr. Ravinder Kumar Sehgal²

¹Computer Science & Engineering, BBSBEC Fatehgarh Sahib Punjab, INDIA.

²Principal, JSSIET Kauli Patiala, Punjab, INDIA.

Abstract: As modern banking increasingly relies on the internet and computer technologies to operate their businesses and market interactions, the threats and security breaches are highly increase in recent years. So online banking presents challenges to financial security and personal privacy when bank information is compromised by skilled criminal hackers by manipulating a financial institution's online information system. This causes huge financial loses to the banks and customers. To provide customers with secure, reliable ,robust online environment to do online banking the banks should adopt "best of breed " technologies to authenticate customers identities when they logon, to ensure that their data is transmitted securely and reliably .Bank should have best backup and contingency plans and should formulate best security policies and practices. In India the Reserve Bank of India (RBI) the governing body constituted a Working Group to examine different issues relating to internet banking and recommend technology, security, legal standards and operational standards keeping in view the international best practices. This paper tries to explore various of Technology and Security Standards the RBI is recommending to banks for safe internet banking and comparison of ICICI bank, OBC bank and HSBC banks based on the recommendations given by RBI for secure online banking.

Keyword: Online Banking, Security measures, RBI recommendations

I. Introduction

Online banking is defined as the use of Internet as a remote delivery channel of banking system services via the World Wide Web .Banks worldwide are increasingly offering online banking services : customers are transferring money from one account to another, checking their account status or investing in stock from their PCs at home and in the office. With all this money being transferred online, online fraudsters try to intercept financial transactions and turn them to their benefit. Banks and customers worldwide have lost millions of dollars through online fraud [1].

Bank information is compromised by skilled criminal hackers by manipulating a financial institution's online information system, spreading malicious bank Trojan viruses, corrupt data, and impede the quality of an information system's performance..So at present customers can do banking online which is easy and time saving and at the same time they are vulnerable to threats [2] .So one of the major concerns of people with respect to internet banking is the safety related to data of bank account, transactional information and also the access path of their accounts [3]. Even the Reserve Bank of India (RBI) that is the main body, has been issuing various directions and recommendations from time to time to strengthen cyber security of banks operating in India. However, RBI observed that at present some banks do not have proper security policy and methods to monitor the service level agreements with third parties and have inadequate audit trail, so it has issued warning to banks to comply the directions of RBI by Oct, 2012. Further, online banking becomes less secure if users are careless or computer illiterate. An increasingly popular criminal practice is to gain access to a user's finances is phishing and other threats include Pharming, Malware, Viruses, theft of user identity and password through other means etc. So if clients are going to use online banking to conduct financial transactions, they should make themselves aware of the risks and take precautions to minimize them.

II. Literature Review

Researchers, Experts have been giving full attention to subjects about Online banking security, the research include Framework for the Governance of Information Security in Banking System[4] and the security issues Internet banking are facing today and solutions for online banking security threats. TC. Shan and WW. Hua summed up security issues in two categories: system security issues and information security issues [5] and the

corresponding solutions are cryptography, identity authentication and the data transmission protection technology [6][7][8]. Researchers also described current authentication threats and proposed solutions and new authentication protocol for online banking [9][10] and introduced new approaches for online banking security [11]. The survey conducted by Data Security Council of India (DSCI) in 2010 indicates that the focus of the data governance processes so far has focused on integrity of data, but there is a need to increase efforts in the direction of data privacy [12]. Laura Falk *et al.* found that 76% of the sites in their survey suffered from at least one design flaw that are not widely understood, even by experts who are responsible for web security and they present and discussed methodology for testing websites [13]. Kenneth Edge *et al.*, defined attack and protection trees and discussed how they can be implemented in the security analysis of an online banking system to maintain user's trust and confidence in the security of their online bank accounts [14]. Many researchers have done studies of several banks in their countries to compare their systems, but in India research on online banking security is still in its infancy. Till now no comparative study regarding security system of different type of banks has been done in India.

III. Internet Banking Security Controls And Measures

The Reserve Bank of India (RBI) is India's central banking institution, which controls the monetary policy of the Indian rupee. The Reserve Bank of India (RBI) was established on April 1, 1935 in accordance with the provisions of the Reserve Bank of India Act, 1934. RBI acts as a banker to the Government and Banks.

Government has taken bold steps since 1991 to give banking a whole new shape. Reserve bank of India (RBI) had set up a 'Working Group on Internet Banking' to examine different aspects of Internet banking. The Group had focused on three major areas of Internet banking, i.e., (i) technology and security issues, (ii) legal issues and (iii) regulatory and supervisory issues. These issues are addressed in lieu with Information Technology Act 2000 [15]. According to RBI report, security of online banking transactions is one of the most important areas of concerns to the regulators. Security issues include questions of adopting internationally accepted state-of-the-art minimum technology standards for access control, encryption / decryption (minimum key length etc), firewalls, verification of digital signature, Public Key Infrastructure (PKI) etc. The regulator is equally concerned about the security policy for the banking industry, security awareness and education. So the information systems security could be achieved by implementing a suitable set of controls which consists of policies, practices, procedures, organizational structures, hardware and software functions. Each organization has to establish these controls to ensure that its security requirements are met [15].

A. Recommendations Of RBI

Reserve Bank of India constituted a Working Group to examine different issues relating to online banking and recommend technology, security, legal standards and operational standards keeping in view the international best practices. The Group is headed by the Chief General Manager-in-Charge of the Department of Information Technology and comprised experts from the fields of banking regulation and supervision, commercial banking, law and technology. The Bank also constituted an Operational Group under its Executive Director comprising officers from different disciplines in the bank, who would guide implementation of the recommendations. This group also recommend minimum technology and security standards, in conformity with international standards and addressing issues like system vulnerability, digital signature, information system audit etc along with other aspects of banking.

RBI has given recommendations for Information Security Policy, which is a documented business rule for protecting information and the systems which store and process this information and security organization, Access Control, Firewalls, Intrusion Detection Systems, Backup and Recovery, Physical Access Controls, Maintenance of infrastructure and monitoring against threats and also given stress on education and training of staff and also time to time guidance and instructions to users.

IV. Comparison of various banks based on RBI security and control recommendations

The major participants in the financial system are the commercial banks, the financial institutions (catching FI's), non-banking financial companies (NBFCs) and other market intermediaries such as stockbrokers and moneylenders. Banks are divided into public sector commercial banks like OBC, State Bank of India, Punjab National Bank, private sector banks like HDFC, ICICI etc and foreign banks like HSBC bank, Citibank, Standard Chartered bank. Internet banking in India emerged in the mid nineties when the newly introduced private sector banks came up with a new business model revolving around a strong information technology (IT) backbone. ICICI bank, a private-sector bank, was the first bank to offer the internet banking

facility to their consumers in 1998. Since then, a large number of both private as well as government banks have opted for offering internet banking services[16].

A. OBC Bank India

Oriental Bank of Commerce (OBC) one of the public sector banks in India was established on 19th Feb' 1943. The Oriental Bank of Commerce was nationalized on 15th April 1980, and paved its way to count amongst the strongest banks in India [26]. As on March 2013, OBC has a network of 2000 branches and 1452 ATM's which includes 1087 Onsite ATMs, 352 Offsite ATMs and 13 Mobile ATMs, spread throughout India. With addition of 1.11 lakh new customers during the year, the Internet Banking customer base has reached to 5.57 lakh [17].

Privacy Policy OBC bank Privacy policy last updated on 09 Oct., 2012. In its Privacy Policy bank has strongly committed to protect the privacy of its customers and taken reasonable measures to protect the security and confidentiality of customer information. Bank uses a strong encryption mechanism, for the transmission of information, which is an accepted and permitted level of encryption in India.

Committee for Security Pursuant to RBI Working Group Information Security recommendations vide Circular No. RBI/2010-11/494 DBS.CO.ITC.BC. No.6/31.02.2008/2010-2-11 dated 29.04.2011, IT Committee of the Board was renamed as IT Strategy Committee in the Board Meeting dated 30.01.2012. The Committee comprises of Chairman and Managing Director, Executive Directors. Bank. During the year IT Committee met four times regarding bank's information security issues and new technology advancements [17].

Access Control 2nd factor authentication based on tracker-Id has been made mandatory for 3rd party fund transfer for Inter & Intra Bank Internet Banking and e-Commerce transactions.

mFacility launched for Online Generation of Login and Transaction passwords for net banking customers. mSecurity features like SMS based Tracker-ID for online transactions and entering password by Net Banking customers after recognizing the personalized image and personalized text appearing on screen on entering the user ID, have been implemented. To further strengthen the access level security for CBS users, bank has started implementing additional biometric authentication wherein the system authenticates the user through his finger prints in addition to user id and password. Bank has implemented Biometric Authentication for users in CBS environment and the same has been operationalised across 900 Branches[17].

Network Oriental Bank has robust, secured and efficient Enterprise Wide Area Network covering approx. 2115 locations. This Network is primarily a Leased Line Based Network. This Network is primarily a Leased Line Based network with ISDN as a backup. The network is three-tier architecture viz. core, Aggregation & access layer. Near Line Site(NLS) at vashi, Mumbai connected to DC through Optical Fiber.

Security Infrastructure: Secure Socket Layering (SSL) protects all data transmissions between your PC and banks' computer system. SSL utilizes authentication and encryption technology developed by RSA Data Security, Inc. Perimeter Security devices have been deployed by OBC to secure the data.

Network security/Firewall Banks computer system does not connect directly to the Internet. Any and all requests for data must pass through two distinct validation and control centers also known as Firewalls.

Penetration Testing The Oriental Bank's iBanking system has been subjected to stringent security reviews and penetration tests by an independent firm. VeriSign Global Secure Site IDs used by the bank enable secure online communications through Secure Sockets Layer (SSL) technology. Global Secure Site Iork. Perimeter Security devices have been deployed to secure the DATA.

Backup/Recovery Bank has implemented-3-way DR architecture through Primary Data Centre, Near Line Site at Mumbai and Disaster Recovery Site at New Delhi for Zero Data Loss for CBS operations. The data is synchronously replicated from PDC to NLS and is asynchronously replicated from PDC to DRS. The Bank has successfully conducted DR Drill during last quarter of 2012-13 to ensure readiness to commence operations through DR in case of an eventuality leading to non-availability of services through Primary Data Centre[17].

Monitoring Against threats Bank has put in place state of the art security equipments and monitoring devices at its Primary and Secondary Data Centers. The security, events are monitored on 24x7x365 basis. The Bank's Data Centre and DIT have achieved ISO 27001:2005 security certification, a highest security standard for Information Security Management System (ISMS) accreditation in the Ministry of Information Technology, Govt. of India, thereby ensuring that Bank adopts contemporary IS Security setup[17].

IT Education to Staff Bank has taken major initiatives to train its staff on various aspects of Banking including training on latest IT Products. E- Learning modules have been created for online learning by the staff through Banks web portal, thereby improving the opportunities to the staff for further up gradation of their skills on various Banking and related activities at their work place[17].

Maintenance of Infrastructure Integration & Maintenance of Web Application Firewall and Database Activity Monitoring and Prevention Security Tool for strengthening Security for Web Based Applications and other related Data is done on regular basis by bank from the third party.

B. ICICI Bank

ICICI Bank was a very early mover in the internet banking space, not only the first bank to introduce this service in India way back in Oct1997, but one of the pioneers in Asia Pacific as well[18]. ICICI Bank, India's second-largest bank with a network of about 2750(540) branches and offices and over 9,000 ATMs. ICICI have leveraged technology to enhance customer convenience. Since the first Internet bank of INDIA was ICICI in 1996, Internet banking as an important mean of providing financial service in IT economic time, is leading to a revolution in banking. However, the computer network has an open resource-sharing architecture, with its original security has congenital demerits. Thus the combination with the modern information technology, the security of banking business inevitably faces the problem. So ICICI Bank's Internet Banking provide a security mechanism to conveniently and securely manage the finances of clients from your home or office.

Privacy Policy The ICICI bank's security policy covers Internet, password, logical access, disaster recovery, Internet messaging, database, application, operating systems,, network, physical, anti-virus, wireless as well as freeware and shareware usage and among other things. Privacy policy also includes what things are expected from clients along with the security mechanism provided by bank. Murli Nambiar, Head- Information Security Group of ICICI Bank says, "Many areas are covered but at present the top priorities in the security policy are logical access, password, application, database, operating system and network." ICICI bank has published its Privacy Policy on website for customers and bank site display that on July, 2012 it was amended last time.

Committees for security ICICI bank has fraud Monitoring Committee that monitors and reviews all frauds involving an amount of ` 10.0 million and above so as to identify the systemic lacunae, if any, that may have facilitated perpetration of the fraud and to put in place measures to rectify the same, identify the reasons for delay in detection, if any, report to top management of the Bank and RBI, monitor progress of investigation, and recovery position, ensure that staff accountability is examined at all levels in all the cases of frauds and action, if required, is completed quickly without loss of time and review of efficacy of the remedial action taken to prevent recurrence of frauds, such as strengthening of internal controls and putting in place other measures as may be considered relevant to strengthen preventive measures against frauds[19].

Access Control ICICI Bank has triple password control strategy that includes, the log-in password and transaction password and grid security. For the funds transfer, users need a separate transaction password. Grid authentication is an enhanced security feature for safeguarding transactions against phishing attacks and frauds. The grid values are indicated on the reverse of Business Banking Card (BBC).

So ICICI Banking involves:

Something the user know: log-in password, Transaction Password

Something the user has: ATM Card, BBC Card

Something the user is: No biometrics is used for user's authentication for doing transactions. But biometrics was implemented last year for critical departments. This has helped reduce user ID and password sharing.

Network The ICICI Bank's network follows a hub and spoke architecture—a mix of VSATs, leased lines, ISDN and radio links. It has around 800 leased lines, about 600 VSATs, approximately 800 ISDN lines and multiple 34 Mbps lines. The network supports the ICICI group offices, banks, branches, and over 1000 ATMs. There are around eight hub locations, which have 3, 4 or 8 Mbps lines as per the requirements for connecting to the branch and regional offices. High-end Cisco routers and switches have been deployed for connectivity [20].

Network security/Firewalls ICICI Bank firewalls is designed to securely separate the Internet from the bank's Internal Web servers, computer systems, networks and databases[8]. The network is monitored using HP OpenView and CiscoWorks. Over 30 portals are operating using a highly secure state-of-the-art security architecture, which consist of firewalls, intrusion detection systems, virus protection and various other tools[20]. The system security is audited by KPMG. Critical systems are audited every year by the bank's internal audit department while external audits are conducted by one or two of the Big Four consulting firms and a regulatory body. In the ICICI bank penetration testing and vulnerability assessment (VA) are done as and when required. The security operations group monitors the status of all devices, hacking attempts and Denial of Service (DoS) attacks and ensures that systems are available and not compromised.

Back up & Recovery The ICICI bank's primary production site is at Mumbai and disaster recovery site (the secondary site) is located at ICICI towers in Mumbai and is used for replication of data. Two centers which are 25-30 Km apart are linked with two 34 Mbps leased lines. To ensure reliability and 24x7 availability, the leased lines pass through separate exchanges [20]. Hardware at both these sites varies from low-end NT servers to the high-end SUN E 10K along with 12 terabytes of data storage at each end connected through a SAN. The group's facilities management team manages over 9,500 desktops, 500 servers and works around the clock.

Monitoring against threats The ICICI bank has also deployed a desktop management suite which helps the IT team scan the environment for deviations and take corrective action. This helps identify discrepancies and

violations of security policy, check for spyware and adware, block device ports (USB, Infrared, Bluetooth) from a central console and check for policy non-compliance on servers.

Education & Review ICICI Bank's security team consists of security professionals in IT teams. Periodic training programs are conducted for the security team, class room training for all IT administrators and system and application owners is also carried out. [19].

Maintenance of Infrastructure The company has its own Security Operations Centre which is manned 24X7. The security operations group monitors the status of all devices and ensures that systems are available and not compromised. Some aspects which the group monitors are hacking attempts and Denial of Service (DoS) attacks.[22].The bank uses standard messaging software and it has blocked freebies.

C. HSBC Bank

HSBC the worldwide bank which is named after the founding member, the Hongkong and Shanghai Banking Corporation Limited, which was established in 1865. The purchase of Marine Midland Bank, US (in the 1980s) and Midland Bank, UK (1992) made HSBC a universal bank. After acquiring the full ownership of Midland Bank, HSBC made the headquarters in London IN 1993. Its international network comprises around 7,200 offices world-wide .In 1959 the acquisition of The Mercantile Bank of India by Hongkong and Shanghai Banking Corporation Limited laid the foundation for HSBC in India with its registered office in Mumbai. HSBC in India is proud to have retained the Group's pioneering streak by being an active partner in the development of the Indian banking industry - even giving India its first ATM way back in 1987. The bank has a network of about 50) branches and offices and 143 ATMs in India.

Privacy Policy Bank's security standards and principles are laid down in the group's IT security Policy and standards. The security standards are consistent with best industry practices including ISO 17799 and relevant regulatory requirements in the markets. Overall responsibility of these standards is given to Group's chief Operating Officer but Group Head of IT has responsibility on day-to-day basis to provide suitable framework for the management of security risks .Periodic reviews and revision are scheduled based upon the input of business and IT security professionals which are located in the principal regions where the group operates.

Committee for Security For establishment, monitoring and periodic review of policies and procedures HSBC have IT security group. The group Chief Operating officer has overall responsibility that standards should be consistent with best industry practices and regulatory requirements in markets. Group Head of IT Security has day to day basis responsibility for policy and for ensuring it continues to provide suitable framework for the management of security risks. IT professionals located in the principal regions advise management on IT security issues and they also have mandate to perform Independent security reviews of internet applications.

Access Control For log on to Internet banking account there are two options in HSBC bank:

Login with Passwords ,

LoginwithSecurityDevice

To log on to Internet Banking account without the Security Device user has need to create a Secondary Password. Once created this Secondary Password user can then use it along with existing Internet Banking User ID and password to log on to user's Internet Banking account. Now user can perform functions like checking account balance, paying utility bills, viewing e-statements etc, by logging on to Internet Banking account with Secondary Password. While making it more convenient for user to log on to HSBC's Internet Banking account, bank endeavor to ensure that the level of safety offered by the Security Device is not compromised. Hence, user will still need Security Device to access certain services such as Third Party fund transfers, Demand draft/Cashiers order request, new cheque book request etc. So financial information is protected by a sophisticated combination of a unique Username and Password, and a one-time Security Code generated by user's Online Security Device.

Network security/Firewall HSBC has implemented industry standard firewalls and network intrusion detection system(NIDS and host based intrusion detection system(HIDS))which are monitored 24 hours a day and 7 days a week by security engineers and security monitoring group. All servers are loaded and configured according to standard build requirements, including standard security toolkit.

Penetrating Testing Independent third party penetration testing is performed on systems on regular basis, simulating attacks against them in a controlled environment to see how they cope.

Backup/Recovery There are standby sites in Hong Kong SAR, UK and US for back-up and in all major regions including pune in India has software developers are available 24 hours to support for software failure. HSBC possesses a substantial disaster recovery capability and at the core of this capability lies a robust multi-site network architecture with built-in redundancy and load balancing features. HSBC web site has also disaster recovery capability, including a back-up site in a separate physical location.

Monitoring Against threats Bank has 24/7 security monitoring and centralized incident management team. Audit trails for administrative and transactional activities.

Education and Review HSBC places a strong emphasis on training of staff so that that must comply with a comprehensive set of security disciplines to ensure that they operate HSBC's systems securely [21].

V. Comparison of Current Implementation Of Security Mechanisms Of Online Banking –HSBC bank in India , ICICI Bank and OBC Bank

Table I Shows the Security System Comparison of HSBC bank India, ICICI bank and OBC bank

Type of security measures	Implemented or not		
	HSBC in India	ICICI in India	OBC Bank
SSL encrypted transmission	Yes	Yes	Yes
CA certificate of the website	Yes	Yes	Yes
Client certificate	Yes	No	No
Security information authentication	Yes	Yes	Yes
Shielding Phishing Websites	Yes(with webroot)	No	No
Account protection and reminder	Yes	Yes	Yes
Double passwords control	Yes(For login either security device is required or secondary password is required along with password)	No (For login only single password is required but for doing transactions bank has transaction password and grid auth facility and OTP)	No(For login only single password is required but for doing transactions bank has transaction password and OTP)
Card (Auth. With something the user have)	Yes	Yes	Yes
One Time Password	Yes	Yes	Yes
Online Security Device	Yes	No	No
Security Questions and Answers	Yes	Yes	Yes
Biometrics	HSBC is the first bank to install facial-recognition technology at its two new data centres for access control in the UK ,but no biometrics are used in India by bank for access control.	Fingerprint biometrics is implemented for critical departments i.e for access control in network and treasury but no biometrics is used for user's authentication for doing transactions.	Bank has implemented Biometric Authentication for users in CBS environment and the same has been operationalised across 900 Branches
Dynamic password card	No	No	No
Virtual keyboard	Yes	Yes	Yes
Password strength testing	Yes	Yes	No
The replacement policy	Yes	Yes	Yes
Active X control	Yes	Yes	Yes
Automatic log off	Yes	Yes	Yes
Mechanism to freeze the incorrect password	Yes(After three wrong attempts system lockout the access)	Yes(After five wrong attempts system lockout the access)	Yes(After three wrong attempts system lockout the access)
The amount of transactions control	Yes	Yes	Yes
Account information notification via SMS	Yes	Yes	Yes
Firewall	Yes	Yes	Yes
Intrusion Detection Systems	Yes	Yes	Yes
Session Timeouts	Yes	Yes	Yes
Automatic Lock outs	Yes	Yes	Yes
Expiry of user ID	Yes	Yes(After one year)	Yes
Use of cookies	Yes	Yes	Yes
Security policy available on site along with latest date of updation	Yes	Yes	Yes
Backup and Recovery	Yes	Yes	Yes
Monitoring against threats	Yes	Yes	Yes
Education and training of staff	Yes	Yes	Yes
Maintenance of infrastructure	Yes	Yes	Yes

VI. Conclusion

With the development of the security technology and mechanism of the Internet banking, as well as the gradual improvement of the security solutions of the Internet banking systems, the Internet banking is becoming more and more secure. All type of banks in India whether public, private or foreign banks trying to implement minimum security measures recommended by RBI time to time. HSBC in India is proud to have retained the Group's pioneering streak by being an active partner in the development of the Indian banking industry - even giving India its first ATM way back in 1987. HSBC is the first bank in India that is providing Online Security Device to their clients to provide more secure banking. HSBC offer Webroot Secure Anywhere software at no cost to our HSBCnet online banking customers. The Identity Shield protects all the details users share with an internet bank. Identifies if a website you visit is the genuine site making sure it's not a false banking (phishing) site. ICICI was the first bank to initiate the Internet banking revolution in India as early as Oct1997 and thus pioneered the concept of net banking. But at the same time it should be noted that the ICICI Bank is one of the most secure and normative Internet bank of INDIA which secure transactions with login password and transaction password along with grid authentication is an enhanced security feature for safeguarding transactions against phishing attacks and frauds. OBC one of the public banks in India provides secure banking to their clients with login password and transaction password. So every bank is in the race to provide best and secure service to their clients by implementing different security standards and techniques and follow the directions and recommendations of RBI time to time. According to comparison HSBC security mechanisms are best and ICICI India's private bank that is the domestic representative for the most advanced and outstanding Internet banks also provide best security mechanism as compared to public sector bank OBC. But everyday cyber criminals are tries different techniques for getting unauthorized access to finances of financial institutions ,banking customers, so the security precautions level of the Internet banking needs further attention and development.

VII. References

- [1] Paul Jeffery Marshall, "Online Banking: Information Security vs. Hackers Research Paper", *International Journal of Scientific & Engineering Research*, Volume 1, Issue 1, Oct2010.
- [2] Zakaria Karim, Karim Mohammed Rezaul, Aliar Hossain, "Towards Secure Information Systems in Online Banking".
- [3] Internet banking in India, <http://tips.thinkrupee.com/articles/internet-banking-in-india.php>
- [4] Munirul Ula, Zuraini bt Ismail2 and Zailani Mohamed Sidek, "A Framework for the Governance of Information Security in Banking System", *Journal of Information Assurance & Cybersecurity*, Vol 2011, Article ID 726196,
- [5] TC. Shan and WW. Hua, "Service-Oriented Solution Framework for Internet Banking", *International Journal of Web Services Research*, vol.3, issue 1, 2006, pp. 29-48.
- [6] M. Nilsson, A. Adams and S. Herd, "Building Security and Trust in Online Banking. *Conference on Human Factors in Computing Systems*", Portland, USA, pp. 1701-1704, 2005.
- [7] E. Kaynak and T.D. Harcar, "Consumer Attitudes towards Online Banking: A New Strategic Marketing Medium for Commercial Banks", *International Journal of Technology Marketing*, vol. 1, no.1, 2005, pp.62-78.
- [8] K.J. Hole, V. Moen and T. Tjostheim, "Case Study: Online Banking Security. *Security & Privacy*", IEEE, vol.4, issue.2, 2006 April.
- [9] Alain Hiltgen, Thorsten Kramp and Thomas Weigold, "Secure Internet Banking Authentication", *IEEE COMPUTER SOCIETY* 2005
- [10] Xing Fang, Justin Zhan, "Online Banking Authentication Using Mobile Phones", *IEEE* 2010.
- [11] A. Hisamatsu, D. Pishva, G.G.D. Nishantha, "Online Banking and Modern Approaches Toward its Enhanced Security", *ICACT* 2010.
- [12] State of Data Security and Privacy in the Indian Banking Industry DSCI-KPMG Survey by DSCI 2010
- [13] Laura Falk, Atul Prakash, Kevin Borders, "Analyzing Websites for User-Visible Security Design Flaws"
- [14] Kenneth Edge, Richard Raines, Michael Grimaila, and Rusty Baldwin Robert Bennington and Christopher Reuter, "The Use of Attack and Protection Trees to Analyze Security for an Online Banking System", *Proceedings of the 40th Hawaii International Conference on System Sciences - 2007 Air Force Research Laboratory*
- [15] RBI Report on Internet Banking 2000. <http://rbi.org.in/Scripts/Publicationreportdetails.aspx?Id=243#ch6>
- [16] Ankit Kesharwani, IBS, Hyderabad Ritesh Tiwari, "Exploraion of internet banking website quality in India:: AWEBQUAL approach introduction literature review", IBS, Hyderabad in Great Lakes Herald Vol 5, No 1, March 2011
- [17] OBC annual report 2012-2013 // <https://www.obcindia.co.in/obcnew/site/SiteSearch.aspx?q=annual%20report>
- [18] Finacle connect published by Infosys Technologies Lt. Feb-April 06 / Vol 01 / Issue 05
- [19] 18th Annual Report and Accounts 2011-2012 Next Generation Banking pioneering Cover Stories: ICICI BANK, Network Magazine issue jan2007. // <https://www.networkmagazineindia.com/200701/coverstory02.shtml>
- [20] Case study: ICICI Centralizes Applications, Network Magazine issue sep 2002, <http://www.networkmagazineindia.com/200209/case1.shtml>
- [21] HSBC Corporate Socia Responsibility Report 2005
- [22] ICICI Bank 1999-2000 Sixth Annual Report.
- [23] Guoling Lao, Xinwang Wang, "Study of Security Mechanisms in Personal Internet Banking - Take China Merchants Bank as an Example", *IEEE* 2010.