International Research Journal of Management and Commerce
ISSN: (2348-9766)
Impact Factor- 5.564, Volume 4, Issue 10, October 2017
Website- www.aarf.asia, **Email** : editor@aarf.asia , editoraarf@gmail.com

STUDY OF ONLINE BANKING SECURITY MECHANISM IN INDIA: TAKE ICICI BANK AS AN EXAMPLE

M. Manidayanand[1], Dr. K. Neelamegam[2]
[1]Research Scholar, Thanthai Hans Roever College of Arts & Science
Elambalur (Post),Perambalur - 621 212
[2]Research Advisor and Convener Assistant Professor in Commerce
Government Arts and Science College, Veppeanthattai, Perambalur- 621116

ABSTRACT

Internet banking has gained wide acceptance internationally and seems to be fast catching up in India with more and more banks entering the fray. online banking is defined as the use of Internet as a remote delivery channel of banking system services via the World Wide Web. This system enable customers to access their accounts and general information of bank products and services anywhere anytime i.e the model of banking has transformed from brick and mortar to all pervading through 'Anywhere and Anytime Banking' through PC or other intelligent device using web browser software, such as Netscape Navigator or Microsoft internet Explorer or Firefox. But Online banking continues to present challenges to financial security and personal privacy. Billions of financial data transactions occur online every day and bank cyber crimes take place every day 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.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.The paper starts from the security problems Internet banking are facing,tries to explain suitable set of controls which consists of policies, procedures, organisational structures, hardware and software functions organisation has to establish , tries to explore various of Technology and Security Standards the RBI is recommending to banks for safe internet banking and analyses the current representative of the online banking security controls and measures with the case of ICICI Bank of INDIA.

Keywords: Online Banking,Security threats,Security measures,RBI

INTRODUCTION

Banking is one of the oldest professions known to mankind. It has undergone many a transition and internet banking is the latest in the list of such transformations. Internet banking has brought about a 360 degree change in the entire banking industry. Such is the change in scenario that timing is no longer a constraint and you can finish your day-today chores and bank leisurely when you have the time i.e its 24 X 7 service. First introduced in the early 1980s (Kalakota and Whinston, 1997), online banking provides its consumers with an application software program that operates on personal computer (PC) which can be dialed into the bank via a modem, telephone line and operated the programs remotely on the consumer PC. Information technology (IT) was primarily employed to automate the back-office (core process and support process) of banks in 1960s.

Nonetheless, enhanced technology was deployed to extend the back-office to the front office (integrated system). This extension helps to enable the banking industry to offer their services via the Internet. The first Internet bank in the world is Security FirstNetwork Bank (SFNB), which was founded in U.S, 1995.Since then, the Internet banking has been rapidly developing around the world, becoming one of strategic points for the commercial banking development.

This method has also made shopping and bill payment,loan payments very easy and convenient. Long queues for these activities have now become history.So online banking or internet banking in simple terms it does not involve any physical exchange of money,but it‘s all done electronically, from one account to another using internet any time anywhere.

Online Banking Security Problems

Billions of financial data transactions occur online every day of the year 24 hours a day 7 days a week and bank cyber crimes take place every day when 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. Cyber crooks, network hackers, cyber pirates, internet thieves is an emerging crime category of criminals and threat to online banking information security systems. According to reports $268 million dollars was stolen online from financial institutions, 2009 cyber-robbery of financial institutions escalated to $559 million dollars (Bankrate.com). If sensitive information regarding commercial and personal banking accounts is not better protected, cyber thieves will continue to illegally access online financial accounts to steal trillions of dollars plus sensitive customer information globally. So online banking continues to present challenges to customer‘s financial security and personal privacy[1]. 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].Millions of people have had their checking accounts compromised, mainly as a result of online banking .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 (account number, PIN etc) 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, Indian banks are not following the directions of RBI in this regard and a majority of banks in India still do not have a well defined cyber security policy. 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, whereby the user is in some way persuaded to hand over their password(s) to a fraudster 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

themself aware of the risks and take precautions to minimize them.

Researchers,Experts have been giving full attention to subjects about Online banking,the research include the issue of Internet banking risk control [4][5], the information technology support and architecture of Internet banking[6][7] , the customer behaviors and trust problems about Internet banking[8][9][10] ,Framework for the Governance of Information Security in Banking System[11] and so on. What worth our concern, many studies have inevitably involved with the security issues Internet banking are facing today and solutions for online banking security threats. The security issues can be summed up in two categories: system security issues and information security issues[12] . And the corresponding solutions are cryptography, identity authentication and the data transmission protection technology[13][14][15].Researchers also described current authentication threats and proposed solutions and new authentication protocol for online banking [16][17]and introduced new approaches for online banking security[18].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 case study regarding security system of different type of banks has been done in India.

II.ICICI Bank

The major participants in the financial system are the commercial banks, the financial institutions (FI's), non-banking financial companies (NBFCs) and other market intermediaries such as stockbrokers and moneylenders. Further commercial banks are divided into public sector commercial banks like State Bank of India, Punjab National Bank, private sector banks like HDFC, ICICI etc and co-operative 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 examines different aspects of Internet banking. The Group had focussed 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[19].

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[20](Infosys Technologies Lt ,2006).ICICI Bank has been following a multi-channel multi-product retail strategy with Internet banking being an integral channel of customer interaction.

ICICI Bank, India's second-largest bank with a network of about 2750(540) branches and offices and over 9,000 ATMs offers banking products and financial services to corporate and retail customers through a variety of delivery channels. ICICI have leveraged technology to

enhance customer convenience and customer experience across a range of channels including ATMs, mobile banking and internet banking[21]. ICICI Bank is the first and only bank in India

to have introduced a powerful new 'Bank Application' on its official Facebook page. Hosted on secure ICICI Bank servers, the application allows customers to access their bank accounts

without having to leave Facebook.They can complete tasks like viewing account details, mini statements, requesting for a cheque book,applying for a debit card and so on, within a familiar and frequently visited environment. Since the first Internet bank of INDIA was ICCI 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 securekly manage the finances of clients from your home or office.

III. Internet Banking Security Controls And Measures:ICICI Bank a case study

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, organisational structures, hardware and software functions**.** Each organisation has to establish these controls to ensure that its security requirements are met[19].

Information Security Policy(IT Vision of Reserve Bank India - 2011-17)

Information Security Policy is a documented business rule for protecting information and the systems which store and process this information. Within an organization, the written policy document provides a high-level description of the various controls the organization will use to protect information. The strength of any system is no greater than its weakest link. Information should be based on the principles of integrity, reliability, and validity. Protecting confidential information is a business and legal requirement.

The existing IS policy would have to be reviewed and updated at periodical intervals. The IS Policy may detail principles for protecting information from unauthorised access, use, disclosure, disruption, modification or destruction. The information security policy should, inter alia, relate to policies such as firewall, email, network security, and password. The policy should also address issues relating to prevention of cyber attacks by deploying appropriate technologies such as two-factor authentication.Structured, well defined and documented security policies, standards and guidelines lay the foundation for good information systems security and are the need of the hour. The Board of Directors/Management of each organization has the responsibility for ensuring appropriate corporate policies, which set out the management responsibilities and the control practices for all the areas of information processing activities. A well-defined corporate security policy has to be put in place and periodically reviewed and amended, as required, under the approval of the Board of Directors/Management.

The ICICI bank's security policy covers Internet, password, logical access, disaster recovery, Internet messaging, database, application, operating systems, intranet, 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.[ii]ICICI bank has published its Privacy Policy on website for customers and bank site display that on july,2012 it was amendend last time.

Security Systems(Hardware and Softwares)

Numerous transactions are carried out on a daily basis hence it's necessary for the bank thave propersecuritysystems that secure its assets from internal and external threats. Some of the measures taken by ICICIbank are:

- Firewalls, intrusion detection systems,Switches, anti-virus as well as routers to secure the perimeter..
- Application security is reviewed periodically, every application undergoes an assessment before implementation in production
- Encryption for desktops and laptops to secure data being carried out on media.
- Biometrics was implemented for critical departments. This has helped reduce user ID and password sharing.
- The Wireless LAN (WLAN) is secured with encryption and only authenticated users are permitted to use the ICICI Bank wireless network
- The bank has 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 noncompliance on servers. Using the software they also conduct vulnerability Assessment (VA) and patch management on desktops and servers to keep them updated with the latest security patches, helping to reduce risks involved with insecure systems being exploited.

The bank uses standard messaging software that eliminate the risk of using free software which provides

various features other than messaging and may be detrimental to the bank's security.

Committees for security

Fraud Monitoring Committee:The Fraud Monitoring Committee currently comprises six Directors including four independent Directors. The Committee is chaired by V. Sridar, an

independent Director. The Committee 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[22].

Information Technology Strategy Committee:The Board of Directors at its Meeting held on September 15-16, 2011 constituted Information Technology (IT) Strategy Committee effective October 31, 2011.The IT Strategy Committee currently comprises four Directors including three independent Directors and the Managing Director & CEO. The Committee is chaired by Homi Khusrokhan, an independent Director .The Committee is empowered to approve IT Strategy and policy documents, ensuring that IT strategy is aligned with business strategy, reviewing IT risks, ensuring proper balance of IT investments for sustaining the Bank's growth, overseeing the aggregate funding of IT at a Bank-level, and ascertaining if the management has resources to ensure the proper management of IT risks and reviewing contribution of IT to businesses[22].

Information Security Governance:In ICICI Bank the Information Security committee or Deputy Managing Director reviews security policy changes and approves the same. The Information security committee consists of senior management from technology and operations.The senior department heads, sign the IT risk management framework which covers threat, vulnerability and impact as well as residual risk. Significant changes to systems are reviewed for changes in the risk profile and the IT security policy is reviewed on a yearly basis and audited for effectiveness on a monthly basis. Security standards are defined in the bank for all systems or technologies and deployed across systems. Murli Nambiar is the Head, Information Security Group.

IV.Technology And Security Standards Of RBI: ICICI bank a case study Security Infrastructure: PKI the strongly recommended technology for secure Internet banking

services,but yet no Certification Authority in India offering Public Key Infrastructure ,so during the transition period, until IDRBT or Government puts in the PKI infrastructure,the usage of SSL and use of at least 128-bit SSL is must.As per requirement ICICI Bank has

- SSL encrypted transmission- ICICI Bank uses 128 bit Secure Socket Layer (SSL) Encryption for information
  transmitted during an Internet Banking session, which is accepted as the industry standard for encryption.
- CA certificate of the website.
- Security information authentication.
- Shielding phishing websites.
- Account protection and reminder.
- Client certificate-Bank don‘t have client certificate.

Access Control

- Double passwords control- ICICI Bank has triple password control strategy that includes, the log-in password and transaction password and grid security.Log-in password requires a mixture of numbers and letters, which means confidentiality in certain degree, and it is limited to log in. 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). To authenticate the transactions, client needs to input some required grid values. In case client do not have a grid-based BBC, clientis prompted to enter random digits of card number to authenticate the transaction.Setting double passwords can effectively prevent the security threats posed by the disclosure of one password.And Grid security prevent the threat of password disclosure by something the user has i.e card.

So ICICI Banking involves:

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

Something the user has:ATM Card,BBC Card

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

- 3D Secure (Verified by Visa (VbV)/ MasterCard SecureCode (MCSC))-In event of anyunusual activity e.g change of IP address etc in your Internet Banking access pattern, 'i-safe' will generate One Time Password (OTP) that will be sent to your mobile number / e-mail ID* registered with us. Authenticating the OTP on Internet Banking 'One Time Password Authentication' page is mandatory to access your account online. Based on a Reserve Bank of India mandate, ICICI bank has introduced an additional layer of security for IVR transactions on ICICI Bank Credit Cards.This means that every time you pay for a purchase or service through any merchant‘s telephone system (IVR), you will be asked to input a One Time Password (IOTP)[10].
- Online Security Device-. The Online Security Device generates a time-sensitive, single-use few digits Security Code to use when logging on to Internet Banking and for selected online transactions. This device provide higher layer of security. No such device is provided by ICICI bank.
- Virtual keyboard.- Virtual Keyboard is an online application to enter password with the help of a mouse. ICICI Bank provides Virtual Keyboard to protect passwords from malicious ¯Spyware‖ and ¯Trojan Programs and to reduce the risk of password theft.
- Password strength testing –Bank‘s site has password strength testing mechasim to give users an idea about how easily password can be guessed.
- Password replacement policy- To prevent unauthorised usage of lost / misplaced Internet Banking user ID / passwords , ICICI Bank disable that immediately after getting information regarding that.Passwords also can be re-issued upon request, and can be generated by internet banking password online..
- Active X control.
- Automatic logout(overtime)-This security features protect us once you have logged in successfully. To protect our accounts against unauthorised access, ICICI bank systems are designed to terminate a secure online session automatically if extended inactivity is detected. Hence if user login and leave his session inactive for 10 minutes , the session will be terminated. In such a situation , user can login again to continue hisr activities.In addition, after logging into icicibank.com, the 'Back', 'Forward' and 'Refresh' buttons of your browser cant be used. If any of these buttons is clicked, secure session will be logged out automatically. This is done to ensure that no unauthorised entry is made

into online account during absence from computer system.

- Mechanism to freeze the incorrect password- After three unsuccessful attempts to login, the user ID will be blocked by banking system automatically. The user id and password will be enabled only on calling our 24- hour Customer Care. After authenticating , user can place his request for re-activation of his user ID. User would be intimated on his registered mobile number about this.
- Expirey of User ID- Internet Banking user ID expires if it is not used for a period of more than one year
- The amount of transactions control- In the ICICI bank, transfer of fund is done through two basic modes. Real Time Gross Settlement is a mode where the transaction to an account takes place more spontaneously (quickly). There are certain minimum limits (Rs 2 lakh) above which this mode of transaction can be used. The other mode is National Electronic Funds Transfer (NEFT) and this mode of transaction takes place in batches (batch of transactions say 4 or 5) in specified regular intervals of time.
- Account information notification via SMS.
- Biometrics- Biometric identification enables authentication of a person on the basis of their personal and individual physical traits such as veins, face recognition or fingerprints.In the bank no such type of identification is used for login and transcation processing.But Biometrics was implemented for critical departments which has helped reduce user ID and password shar**ing**

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 is a primary site from where spokes go out to the regional branches and the other offices. The secondary site has the disaster recovery system.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

3G Network security/Firewalls

One of the security mechanisms used to protect banks systems and customers information is called a firewall.ICICI Bank firewalls use a combination of industrial strength computer hardware and software that is designed to securely separate the Internet from the bank‘s Internal Web servers, computer systems, networks and databases. During customers secure online sessions with RBC Web sites, firewalls prevent unauthorized Internet traffic from entering banks‘s Web servers, systems and network[8]. So, to protect data stored on bank‘s systems and to prevent unauthorised access,bank employ firewalls where ever appropriate. 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[21].

- Isolation of Application Servers: It is also recommended that all unnecessary services on the application server such as ftp, telnet should be disabled. The application server should be isolated from the e-mail server.An open source FTP server application has been customised to meet the requirements of the ICICI bank. The internet banking service has isolation of web servers[23].
- Security Log (audit Trail): According to RBI , all computer accesses, including messages received, should be logged. All computer access and security violations (suspected or attempted) should be reported and follow up action taken as the organization‘s escalation policy. The auditors conduct physical tests of the systems wherein tools such as desktop management tool are used to scan for viruses and apply security patches for desktops, laptops and servers. 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. Using the software they also conduct vulnerability Assessment (VA) and patch management on desktops and servers to keep them updated with the latest security patches, helping to reduce risks involved with insecure systems being exploited.The security cell has developed several tools, which are the first of its kind to address several vulnerabilities on Unix, NT and MS-

Exchange. 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.

Penetration Testing

In the ICICI bank penetration testing is executed for all Web based systems . Penetration testing (PT) and vulnerability assessment (VA) are done as and when required. They change the vendors involved every year. The security operations group monitors the status of all devices and ensures that systems are available and not compromised.The group also monitors the hacking attempts and Denial of Service (DoS) attacks.

Back up & Recovery

An off-site back up is necessary for recovery from major failures / disasters to ensure business continuity.So the bank‘s main production site is at Mahalaxmi, Mumbai (the primary site), and has been built to international standards. The disaster recovery site (the secondary site) is located at ICICI towers in BandraKurla complex, Mumbai and is used for replication of data. A distance of 25-30 kms separates the two centers and they are linked with two 34 Mbps leased lines. To ensure reliability and 24x7 availability, the leased lines pass through separate exchanges[21].

Before the data moves on to the leased lines, it passes through two CNT storage directors that convert this data into WAN-related traffic before it is sent on the leased line to the other data center. The high-speed leased lines make it possible to synchronize data in real-time between the two centers[21].

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. CA Unicenter is used for managing the helpdesk, desktops and servers, asset management, software delivery and remote control.

Monitoring against threats

The banks should acquire tools for monitoring systems and the networks against intrusions and attacks. These tools should be used regularly to avoid security breaches. 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

The banks should review their security infrastructure and security policies regularly and optimize them in the light of their own experiences and changing technologies. They should educate on a continuous basis their security personnel and also the end-users.

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. All the web developers are trained on secure coding practice on a yearly basis[22].

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.

The information security officers consist of domain experts responsible for LAN, WAN, Web and database security. The security operations group normally resolves issues and escalates matters to the security officers for second level support. The information security officers escalates the issues to the management if a corporate decision needs to be taken. The 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. Using the software they also conduct vulnerability Assessment (VA) and patch management on desktops and servers to keep them updated with the latest security patches, helping to reduce risks involved with insecure systems being exploited(Network Magazine issue jan 2007, networkmagazineindia. com).

The bank uses standard messaging software and it has blocked freebies. The benefits of using a standard messaging software is to eliminate the risk of using free software which provides various features other than messaging and may be detrimental to the bank‘s security.Banking site works on Internet Explorer Version 5.5 and above Netscape Navigator Version 7.1 and above.

V.Current Implemention Of Security Mechanisms Of Domestic Personal Internet Banking –Take ICICI Bank an Example

Type of security measures	**Implemented or**
SSL encrypted transmission	Yes
CA certificate of the website	Yes
Client certificate	No
Security information authentication	Yes
Shielding Phishing Websites	No
Account protection and reminder	Yes
Double passwords control(Auth. With something	Yes
Card (Auth. With something the user have)	Yes
One Time Password	Yes
Dynamic password card	No
Virtual keyboard	Yes
Password strength testing	Yes
The replacement policy	Yes
Active X control	Yes
Automatic overtime	Yes
Mechanism to freeze the incorrect password	Yes
Graphic verification code	Yes
The amount of transactions control	Yes
Account information notification via SMS	Yes
Firewall	Yes
Intrusion detection systems	Yes
Session Timeouts	Yes
Automatic Lock outs	Yes
Expiry of user ID	Yes(After one year)

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. Security is the basis for the development of Internet banking. Only when the security is fully protected,the Internet bank

can deal with other traditional banking business more. Internet banking has gained wide acceptance internationally and seems to be fast catching up in India with more and more banks entering the fray . The Reserve Bank of India (RBI) that is the main body, issue various directions and recommendations from time to time to strengthen cyber security of banks operating in India.Security issuesinclude adoption of 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 by banks. ICICI BANK has considerable number of types of the security mechanisms to conveniently and securely manage the finances of clients from your home or office in a certain extent.ICICI was the first bank to initiate the Internetbanking revolution in India as early as Oct1997 and thus pioneered the concept of netbanking But at the same time it should be noted that the ICICI Bank is one of the most secure and normative Internet bank in INDIA which follow all the directions and recommendations of RBI time to time.Its security mechanisms are perfect and it is the domestic representative for the most advanced and outstanding Internet banks. 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.

References

[1]. Paul Jeffery Marshall.Online Banking: Information Security vs. Hackers Research Paper,in International Journal of Scientific &

[2]. Engineering Research, Volume 1, Issue 1, Oct2010.

[3]. Zakaria Karim,Karim Mohammed Rezaul, Aliar Hossain.Towards Secure Information Systems in Online Banking.

[4]. Internet banking in India,http://tips.thinkrupee.com/articles/internet-banking-in-india.php S. Laforet and X. Li. Consumers‘ attitudes towards online and mobile banking in China. International Journal of Bank Marketing, vol. 23, no.5, 2005, pp. 362-380.

[5]. Y. Zhu . How to strengthen Internet banking security management.Modern Finance, no. 10, 2006, pp. 32.

[6]. Hossein Jadidoleslamy. Designing a New Security Architecture for Online-

Banking: A Hierarchical Intrusion Detection Architecture and Intrusion Detection System.The Computing Science and Technology International Journal , vol. 2, no. 2, June, 2012.

[7]. Damein Hutchinson,Matthew warren. ,Security for Internet banking:A Framework. Logistic Information Management Vol 16,Number 1,2003 ,pp 64-73.

[8]. M. Mannan and P.C. van Oorschot. Security and Usability: The Gap in Real-World Online Banking. New Security Paradigms Workshop,2007.

[9]. Y. Nie and R. Huang. The risks and control of the Internet banking. Market Modernization, no 8, 2004, pp. 34-35.

[10]. Y. Huang. The research of Internet banking risk prevention strategy. Contemporary Finance, no. 4, 2008, pp. 44-45.

[11]. Munirul Ula, Zuraini bt Ismail2 and Zailani Mohamed Sidek. A Framework for the Governance of

[12]. 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.

[13]. 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.

[14]. 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.

[15]. K.J. Hole, V. Moen and T. Tjostheim. Case Study: Online Banking Security. Security & Privacy, IEEE, vol.4, issue.2, 2006 April.

[16]. Alain Hiltgen,Thorsten Kramp and Thomas Weigold. Secure Internet Banking Authentication, IEEE COMPUTER SOCIETY 2005

[17]. Xing Fang, Justin Zhan. Online Banking Authentication Using Mobile Phones,IEEE 2010.

[18]. A. Hisamatsu, D. Pishva, and G.G.D. Nishantha. Online Banking and Modem Approaches Toward its Enhanced Security, ICACT 2010.

[19]. RBI Report on Internet Banking 2000.

http://rbi.org.in/Scripts/Publicationreportdetails.Aspx?Id=243#ch6

[20]. Finacle connect published by Infosys Technologies Lt. Feb-April 06 / Vol 01 / Issue 05

[21]. case study: : ICICI Centralizes Applications, Network Magazine issue sep 2002,

[22]. http://www.networkmagazineindia.com/200209/case1.shtml

[23]. 18thAnnual Report and Accounts 2011-2012 Next Generation Banking pioneering Cover Stories:ICICI BANK, Network Magazine issue

[24]. jan2007, www.networkmagazineindia.com/200701/coverstory02.shtml

[25]. ICICI Bank 1999-2000 Sixth Annual Report.

[26]. Guoling Lao, Xinwang Wang.Study of Security Mechanisms in Personal Internet Banking - Take China Merchants Bank as an

[27]. Example,IEEE 2010.

[28]. Online Banking: Threats and Countermeasures Revised Version: 1.3 Release Date:June, 2010 AhnLab, Inc.