Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Infrastructure and Security Concerns on Internet Banking in India

Mrs T.K. George
Research Scholar
Cochin University of Science and Technology

Dr Paulose Jacob
Professor
Cochin University of Science and Technology

Abstract - Internet banking is an emerging concept in the banking industry in India for the value added transactions by the banks for their customers. It uses the reliable internet and communication technology to offer the wide range of products and services based on their content and sophistication to reach out to their customers, round the clock, throughout the year. Remote accessing is an added advantage of internet banking. The traditional banking transactions are delivered through the reliable communication backbone, ie. the internet. Vulnerabilities and loop holes in this infrastructure to deal with the diverse hardware and software technologies used by banks may increase the challenges faced by both the bankers and customers, which have to be patched by evaluating the consequences faced by the players of the business and the immediate requirements to support the business strategy and its effectiveness. According to the suggestion made by the Reserve Bank of India, a password based "Two-stage authentication" process and an effective PKI based system can be the most favored technology for increasing the security and reducing the frauds in internet banking, which has not been effectively implemented. Security constraints on SSL have to be verified based on the type of transactions and its sophistication.

Keywords: Internet banking, Infrastructure, Authentication, PKI, SSL

Introduction:

Internet banking portals provide various facilities to its customers to access the information, viz. querying on the transaction details using the existing communication and internet infrastructure available in the country. Security will be an important concern in internet banking, if the providers are using inappropriate technology standards for accessing the details, encryption / decryption system, or protect the communication channel with commonly used firewalls and fraudulent authentication strategies of Public Key Infrastructure. Internet banking can reach out to the customers easily by overcoming the traditional geographical barriers, with a better speed and greater accessibility. In due course of time a new risk of controlling and validating the security and privacy of electronic transaction has risen. Since internet is a public domain, there are different dimensions to tackle the global transactions, which seem to be the problematic issue for the bankers to deal with the security of data and its transmission within the network[1]. Even though these are the common challenges in any closed user groups, the dimensions of the risk is higher over the internet and the prevention or control measures are comparatively fewer. It is important to respond to the technology in time, so as to avoid the strategic risk of losing the customers and the business profit.

The Internet banking facts & concerns:

Security is the primary concern in Internet banking, in comparison with traditional banking transactions. Appropriate technological support is required to transmit the information safely with the required level of integrity of the total transaction management. The security concerns can be addressed at different levels such as security of customer information, Internet banking server with customer database and the malicious attack during the transaction management[2].

Secure Socket layer (SSL) is an important security protocol usually applied to handle the data security between the customer browser and Web server[2]. SSL protocol initiates the connection (client and server agreeing on the level of security to complete the any authentication requirements) with a hand shake signal and provides the Security in data encryption, server authentication, and message integrity for an Internet connection. Online banking application must support data encryption at the highest level to achieve the security in encryption. Internet banking transactions should have a browser that supports this encryption and patches up any security holes in it[3].

Technological support behind internet banking.

- Secured TCP/IP protocol which supports the data packets to transmit between the network with an appropriate cryptosystem, which can be addressed with the support of a Secure Socket Layer[4].An appropriate FTP site which makes the documents accessible for the public by permitting them to use the system by validating the customer ID password. Unique interfacing of their private network to internet can be provided for offering the secured email communication to their customers.

- Usage of HTML to attach the sophisticated credentials that can support the convenient means of navigating through the net.
- Wireless access to the internet by a WAP which supports industry standard for designing applications and other services for wireless services with interactive facilities and sufficient security requirements. This has been a turning point with regard to the commercial use of the internet[5].
-

Indian banks into Internet banking

India can be on the threshold of the banking revolution having many customers showing their interest in Internet banking[2]. It has already gained wide acceptance internationally and is considered as a strategic tool of banking transaction for the future generation, with more banks focusing on the security aspects of the banking transaction. Since the cost of banking services in conventional methods are expensive compared to internet banking, most of the bankers are concentrating on internet channel for providing banking services. In the Indian scenario, ICICI Bank Ltd., Citibank, SBI**,** HDFC Bank Ltd., UTI Bank Ltd., are considered as some of the major players in the internet banking. The HDFC Bank Ltd. has promoted e-shopping and at the same time, online real time shopping malls payments are made by ICICI bank Ltd. Banks in India are adopting internet technologies to attain market supremacy and better business[6].

An analysis on the technological support for Internet Banking

The backbone

Internet banking application can be run on a different security framework and provide various services for both bankers and customers. The important tasks such as user interaction, online transaction processing based on the business rules, business data storage and retrieval can be implemented by using a multi-tier framework[7]. It consists of a presentation layer which deals with session management and interface related issues. There also exists an application layer which is in charge of ensuring the business rules and a data layer which updates, maintains & recovers data.

Security and Privacy Issues

In internet banking, appropriate security of hardware, software and communication technology is essential to preserve the resources against the unauthorized access and preserve the valuable resources from any type of malicious attack or destruction. There should be a proper authentication system to verify the identity of the customer and stop the vulnerable unauthorized entities by using an appropriate crypto system. Malicious users can cause major changes in the system. Discretionary or mandatory access control can be implemented for the effectiveness of the system. An intruder can be the reason for denying the access of a privileged user. In the absence of a properly configured system and lack of security patches, hackers can enter the system through the security holes. With the help of an appropriate encryption & decryption system the confidentiality of the message can be ensured.

PKI plays an important role in supporting the required security services, by way of providing key certificate for the trusted path to support the digital signature to increase the confidentiality of electronic transactions. Security tools scanners, sniffer devices, intrusion detection and other auditing tools can be used for monitoring and controlling users, networks and banking systems[8].

General view on the Support of Security Policies within the Bank

Design & utilization of security policies are important criteria to formulate the information security measures and to protect the system from the vulnerabilities. Some of the general views regarding the security policies are:

- Assign the appropriate priorities for information systems that have to be protected.
- Responsibilities of the management team and their support have to be clearly indicated.
- Cyber security involvement and counter measures to protect the system should be indicated.
- Prior to the implementation of the system risk analysis, an auditing has to be done.
- There should be an appropriate format or procedure and a periodic review for updating the current requirements & security measures.
- Employee’s role & responsibilities have to be indicated with due importance to take care of the system.
- Training and awareness programs have to be conducted.

Recommendations and views on Internet banking & its Security Measures

The most favored supporting technology for internet banking is the Public Key Infrastructure (PKI), which is not easily available. Some of the research report indicates that usually the governments recommend this technology because of its usage of 128-bit SSL for server authentication and the verification of the credentials .The application server should provide only the required services and should be isolated[9]. There should be a provision of appropriate Audit Trail and the security log should be handled carefully. The responsible security officer should conduct penetration test to take care of password-cracking Denial of services, Security holes in the software[10]. Some of these tests can be performed with the help of an 'Ethical hacker'. But appropriate care should be taken for physical access to protect the system from internal and external threats[11].

Back up of data & its recovery after the failure, should be taken care, by providing the required infrastructure and testing it periodically. Security scanning and monitoring system can be placed to take care of the intrusion detection. Training should be provided in a continuous basis for those who handle the technical aspect of the banks, and any changes in security policies have to be informed on priority basis[12]. Only certified products or solutions should be used by the agents to give security patches or to protect the system to have a better control. The banks utilizing internet banking facilities in India, have to obtain an approval from the Reserve Bank of India, by submitting the required documents related to all aspects of security and in return, they must get an operational manual of security frame work[13].

Conclusion

The most important aspect of internet banking is its cost effectiveness compared to the conventional banking. Majority of the banking services are focused on internet facilities to reach their value added services to the customers[14]. Most of them are already equipped with security analyzers and monitors to analyze the unauthorized attempt to log into the accounts to mitigate any types of trapdoor entries and to protect the resources. The importance of secure transactions should be addressed from every angle within the frame work of the internet banking application. Better authentication levels of user data can be carried out by deploying SSL security protocol on the web server, and the proper choice of browser software along with the multitier framework will create yet another firewall to carry out the specific functions on the dedicated network[15]. Keeping a check on the attempts of intruders and taking the customers into confidence by reaching the resources to the most valued customers within a strong internet security frame work, will achieve profit in new generation banking Business. Customers' perception can be changed by awareness programs[16]. Easy and convenient access, required level of security, decrease in transaction costs and timely response to the queries are clear indicators of better adoption of internet banking among the future users of the banking services.

References:

[1].Khan, M S; S. S. Mahapatra and Sreekrumah (2009). Service Quality Evaluation in Internet Banking: An Empirical Study in India. International Journal of Indian Culture and Business Management, 2(1),30 – 46.

`[2] .Mukherjee A and Nath P (2003), "A model of trust in online relationship banking", International Journal of Bank Marketing, Vol. 21, No.1, pp.5-15.

[3] .Nath R, Paul S and Monica P (2001), "Bankers' Perspectives on Internet Banking" e-Service Journal, Vol. 1, No.1, pp.21-36.

[4] .Dhillon, G. (2001) Challenges in managing information security in the new millennium. In G. Dhillon (ed.) Information Security Management: Global Challenges in the New Millennium.

[5] .Dhillon, G. and Torkzadeh, G. (2006) Values-focused assessment of information system security in organizations. Information Systems Journal 16 (3): 293–314.

[6] .Singhal, D and V. Padhmanabhan (2008). A Study on Customer Perception Towards internet Banking: Identifying major contributing factors. The Journal of Nepalese Business Studies. V (1), 101 – 111.

[7]. Beer, Stan (2006). Customers Preference on Internet Banking, Survey (Retrieved from http://www.itwire.com/content/view/4570/53 on March 20, 2009).

[8] .Chaffey, D; Mayer, R; Johnson, K and Ellis Chadwick, F (2006). Internet Marketing: Strategy, Implementation and Practice, (3rd Edition) Financial Times/Prentice Hall, Harlow, Essex, U.K, 8 – 10.

[9] .N. K. Malhotra, S. S. Kim, J. Agarwal (2004), "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model" Information Systems Research, vol. 15, no. 4, pp. 336-355.

[10] .Parker, Donn B., (2004) Toward a new framework for information security, in Computer Security Handbook, 4th edition, Bosworth, Seymour and Kabay, M. E. (eds.), John Wiley and Sons.

[11] .Giannakoudi, S. (1999) 'Internet banking: the digital voyage of banking and money in cyberspace', *Information and Communications Technology Law*, Vol. 8, No. 3, pp.205–243.

[12]. Khalfan.et al,2006, Factors influencing the adoption of internet banking in Oman, a descriptive case study analysis. International Journal of Financial services management. 1(2) 155-172

[13] .Mishra A K (2005), "Internet Banking in India Part-I".

[14] .Mols N P (1999), "The Internet and banks' strategic distribution channel decision", International Journal of Bank marketing, Vol.17, No.6, pp.295-300.

[15] .www.financialexpress.com/fe/daily/19980714/19555264.html (15 Sept. 2010)

[16] .http://www.banknetindia.com/banking/ibkg.html (15 Sept. 2010).