E-Banking Security and Challenges: A Survey

Conference Paper · December 2013

CITATIONS
0

READS
2,756

2 authors:

Krishan Kumar
Gurukula Kangri Vishwavidyalaya
33 PUBLICATIONS **152** CITATIONS
SEE PROFILE

Mohit Mittal
Kyoto Sangyo University
28 PUBLICATIONS **57** CITATIONS
SEE PROFILE

E-Banking Security and Challenges in India: A Survey

KRISHAN KUMAR
Assistant Professor
Department of Computer Science
G.K.V, Haridwar
kumar_krishana@yahoo.com

MOHIT MITTAL
Research Scholar
Department of Computer Science
G.K.V, Haridwar
mittal.mohit02@gmail.com

Abstract- Today, in every aspect of our life, we are using information technology (IT) to make our life comfortable. Banking sector, completely based on the consumer database, using online transactions widely, also affected by IT. Rapid growth of a technology; where the main concerns are related to security and cost, Internet banking – suggests that these concerns can be solved for many aspects like digital sign and electronic signatures as well. In the Internet banking, the web browsers provide simple and user-friendly interface to customers. This paper gives a survey for the required security and challenges faced by all banks in internet banking. Like technology service providers globally have firmed up cloud computing platforms that have opened vistas for agile and cost effective solutions. Prevention of cyber crimes is the main challenge for banks with proper customer service.

I. INTRODUCTION

Due to IT revolution various new technologies are being introduced in production and service sector. IT tools are introduced for the better performance and faster growth rate. With arrival of foreign and private banks with superior technology pushed banks to follow the latest technology to meet the growing competition and retain their customer satisfaction. Now Indian banking industry is in the mid of IT revolution. Rapid growth of a technology where the main concerns are related to security and cost – *Internet banking* – suggests that these concerns can be solved for many aspects like digital signers and electronic signatures as well. The role of Internet is becoming inevitable in a society. The Internet banking is changing the environment of banking industry and is having the major effects on banking relationships [1].

Today, Information Technology (IT) not only facilitates automation of process and data processing but also provides more value addition to the entire banking business. Further, it is directly and visibly linked to 'value to customer'. In such a scenario should IT be delivered and managed within the Bank or outsourced? The key challenge is to proactively respond than be reactive to change. Banks are now expecting outsourced service organizations to proactively sense business needs and change rather than be told to change. While the emergence of communication frameworks has been a boon to business but integration of various structured and unstructured data will be the key for prompt and personalized services. Banks are deploying sophisticated analytical systems to enable personalized communication and services to customers. A bank that communicates well is able to sense and change faster. The Internet motivated many companies to use the Internet to sell products/services online services the Internet users intend to buy. In other words a successful Internet banking solution offers [1]:

- Exceptional rates on Savings, CDs, and IRAs.
- Checking with no monthly fee, free bill payment and rebates on ATM surcharges.
- Credit cards with low rates.
- Easy online applications for all accounts, including personal loans and mortgages.
- 24 hour account access.
- Quality customer service with personal attention.

The paper aims to protect customer's privacy and protect against fraud at providing a specific focus to identify the security issues in banking system also the impact of demographics in influencing Internet users in consuming different services online.

In a survey conducted by the Online Banking Association, member institutions, rated security as the important issue of online banking. There is a dual requirement to protect customer's privacy and protection against fraud. A multi-layered security architecture comprising firewalls, filtering routers, encryption, and digital certification ensure that your account information is protected from unauthorized access. According to the survey conducted by the Internet and Mobile Association of India (IAMAI) there are estimated 20 million Internet users who are banking online now [2].

PC Magazine Online also offers a primer: How Encryption Works. There are some key areas in banking where technology has contributed the most are: Product Development, Market Infrastructure, Risk Control and Market Research [3], [4].

1. Types of Internet Banking

Currently, there are three basic kinds of Internet banking technologies that are being employed in the marketplace are:

- Information,
- Communication, and
- Transaction.

2. The Role of banks in the Internet world

Throughout the country, the Internet Banking is in the ascent stage of development (only 50 banks are offering

varied kind of Internet banking services). In general, these Internet sites offer only the most basic services. 55% are so called 'entry level' sites, offering little more than company information and basic marketing materials. Only 8% offer 'advanced transactions' such as online funds transfer, transactions & cash management services. Foreign & Private Banks are much advanced in terms of the number of sites & their level of development. Internet Banking is the new generation of banking in India. Most private and MNC banks have already setup an elaborate Internet banking infrastructure [1].

Initially, banks promoted their core capabilities, being products, channels and advice, through the Internet. Then, they entered internet commerce market as providers/distributors of their own products and services. "The trend toward electronic delivery of products and services is occurring dramatically in the financial service industry (something we call "e-Finance") where the shift is partly a result of consumer demand, but also of a ruthlessly competitive environment". More recently, due to advances in Internet security and the advent of relevant protocols (e.g. Integrion, OFX, SET etc.), banks discovered that they can play again their primary role as financial intermediates and facilitators of complete commercial transactions via electronic networks and especially via the Internet. However, this scheme is very abstract and vague and does not support any decision-making process for the banking institutions to define a niche market for them to invest on and compare with their rivalries [5].

3. Internet Banking in India

The study, conducted by students of IIML shows some interesting facts. The banking industry in India is facing unprecedented competition from non-traditional banking institutions, which now offer banking and financial services over the Internet. Indian banks are going for the retail banking in a big way. However, much is still to be achieved [2].

The following regulatory and policy constraints apply in India:

Eligibility of clients

Under Reserve Bank of India guidelines, smart or debit cards can only be issued to clients who have maintained their account satisfactorily for six months.

Loading of value

The section on cash withdrawals does not permit the withdrawal of cash or deposit through a POS terminal.

Presence at ATMs

The current guidelines do not allow the presence of any persons other than security guards at ATMs, effectively preventing the bank from providing direct assistance to low-income, frequently illiterate customers.

Written record of transactions- A written receipt is required either at the instance of the transaction or in a regular report.

Customs duties

While automatic teller machines have a customer duty of 60 per cent, cheaper versions (cash dispensers), which have the potential to reach out to the mass market, have a customs duty of 150 per cent.

Service area agreements

The current service area approach restricts competition between banks in rural areas, thus making it more difficult for a bank to strategically roll out networks of ATM machines.

II. PROBLEM STATEMENT

Reserve Bank of India had set up a "Working Group on Internet Banking" to examine different aspects of Internet Banking (I-banking). The Group had focused on three major issues of I-banking:

- Technology and security issues
- Legal issues
- Regulatory and supervisory issues

RBI has accepted the recommendations of the Group to be implemented in a phased manner. Banks are also advised that they may be guided by the original report, for a detailed guidance on different issues [10]. The Internet must be secure to achieve a high level of confidence with both consumers and businesses. So the issues that will help maintain a high level of public confidence in an open network environment include:

- Security
- Authentication
- Trust
- No repudiation
- Privacy
- Availability

1. Risks Involved in Internet Banking

Internet banking risks consists of risk associated with credit, interest rate, transaction, liquidity risk, price risk, transaction risk, etc. Some of the important risks involved in the Internet banking are:

Credit Risk

Customers can reach from anywhere, challenging for institutions to verify the bonafides of their customers, which is an important element in making sound credit decisions.

Liquidity Risk

Increase deposit volatility from customers who maintain accounts solely on the basis of rate or terms.

Interest Rate Risk

Interest rate risk arises from differences between the timing of rate changes and the timing of cash flows reprising risk [6].

Foreign Exchange Risk

Foreign exchange risk is present when a loan or portfolio of loans is denominated in a foreign currency or is funded by borrowings in another currency [7].

Compliance Risk

Compliance risk is the risk to earnings or capital arising from violations of, or nonconformance with, laws, rules, regulations, prescribed practices, or ethical standards [8].

Strategic Risk

Strategic risk is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes [9].

Reputation Risk

Reputation risk is the current and prospective impact on earnings and capital arising from negative public opinion [11].

III. OBJECTIVES OF THE STUDY

The objective of the study is to study and analyze the current issues related to security in online transactions, mobile banking etc. in our Internet banking systems for public banks like State Bank of India, Punjab National Bank, Bank of Baroda. By the year 2013, a large sophisticated and highly competitive Internet Banking Market will develop in a survey conducted by the Online Banking Association; member institutions rated security as the most important issue of online banking. The purpose of this research is to establish the relationship between technology and service quality in the banking industry in India. One of the important areas of e-banking is Mobile Banking, which is being deployed using mobile applications developed on one of the following four channels: IVR (Interactive Voice Response), SMS (Short Messaging Service), WAP (Wireless Access Protocol), Standalone Mobile Application Clients.

In future we have planned to study the various security aspects for internet banking and will try to implement an integrated authentication model by using new technological approach like SSL encryption to deal with security challenges of internet banking system. Moreover, we will propose a multifactor authentication technique that is a digital signer device with biometric authentication that not only provides a tamper proof storage for the digital signature but also provides its own display and keyboard. The motivation of such a system is to escape the scalability and complexity problems that arise if a large-scale Public Key Infrastructure (PKI) is used. This system will improve the security of smart cards by avoiding its dependence on the computer to interface with the user, making it immune to virus attacks and also aging factor of human being.

IV. HYPOTHESIS FORMULATION

It is indeed essential to emphasize the fact that the Indian culture is different from the countries where previous research was conducted. The researchers predicted that the familiarity and economic benefits of using the Internet has a significant impact on the acceptance of online banking. If customers are not used to accessing the Internet frequently, and if they do not trust the Internet as a secure environment to conduct financial transactions, then it is nearly impossible for them to accept online banking. Therefore, the following is hypothesized:

1-Security and privacy has significant impact on adoption of Internet banking.

2-Trust has significant impact on adoption of Internet banking among customers.

3-Innovativeness has significant impact on adoption of Internet banking.

4-Familiarity has significant impact on adoption of Internet banking.

Mostly Internet banking in not being used by general masses because of the lack of awareness among them, in general security becomes constraint to obtaining meaningful data and information. Further, it is very difficult to get data from banking sources due to security reasons. The following organizational aspects should be reviewed for whether:

1-Due diligence and risk analysis are performed before the bank conducts Internet banking activities.

2-Due diligence and risk analysis are performed where cross-border activities are conducted.

3-Internet banking is consistent with the bank's overall mission, strategic goals and operating plans

4-Internet application is compliant with the defined and approved business model.

V. RELATED WORK

The paper articulates the key issues in extending banking to the customers in the country and provides recommendations for the Reserve Bank and the Government of India. While extension of banking services to the poor and rural populations is essential, it is also important to view banking in a new perspective with the advent of new technology [12].

ICICI Bank, India's second largest financial institution, is leveraging new partnerships and innovative uses of information and communication technology (ICT) to profitably market banking services to the poorest of the poor. The bank has combined its capital and expertise with the social mobilization strength of existing microfinance organizations and self-help groups to help such groups scale up their activities [13].

In the recent years there has been explosion of Internet based electronic banking applications. Beckett et al. stated that the emergence of new forms of technology has created highly competitive market conditions for bank providers. However, the changed market conditions demand for banks to better understanding of consumers' needs. The concept of electronic banking has been defined in many ways (e.g. Daniel, 1999) [17], [18], [19].

According to Karjaluoto (2002) electronic banking is a construct that consists of several distribution channels. Daniel (1999) defines electronic banking as the delivery

of bank's information and services by banks to customers via different delivery platforms that can be used with different terminal devices such as a personal computer and a mobile phone with browser or desktop software, telephone or digital television. Electronic banking is also commonly known as Internet banking or e-banking. Internet Banking, also defined as ''the delivery of banking services through the open-access computer network directly to customers' home or private addresses.''[20].

Lau, has experienced phenomenal growth in recent years all over the world. In 2006, Pew Internet and American Life Project reported that nearly half of internet users in the United States were online. In many ways, e-banking is not unlike traditional payment, inquiry, and information processing system, differing only in that it utilizes a different delivery channels. Any decision to adopt e-banking is normally influenced by a number of factors. Liao et al. stressed that the success in Internet banking will be achieved with tailored financial products and services that fulfill customers' wants, preferences and quality expectations [21], [22].

Mattila (2001) concedes that customer satisfaction is a key to success in Internet banking and banks will use different media to customize products and services to fit customers' specific needs in the future. Liao et al. suggested that consumer perceptions of transaction security, transaction accuracy, user friendliness, and network speed are the critical factors for success in Internet banking [23], [24].

Now day's uptake of applications in the e-banking industry is very slow only because of security and data confidentiality issues. Security and privacy are one of the most challenging problems faced by customers who wish to trade in the ecommerce world. Security in the form of keeping customer safe from an invasion of their privacy, affects trust and satisfaction. If company wish to maintain customer trust, they need to keep their promises regarding security and privacy. Since security is closely related to trust, violations of security norms may backfire in terms of losing customers and negative word-of mouth. Security perceptions are defined as "the subjective probability with which consumers believe that their private information will not be viewed, store and manipulated during transit and storage by inappropriate parties in a manner consistent with their confident expectations" (Pavlou 2001).

Dr. David Chaum, CEO of DigiCash said that security is simply the protection of interests. People want to protect their own money and bank their own exposure. With electronic cash, just as with paper cash today, it will be the responsibility of government to protect against systemic risk. This is a serious role that cannot be left to the microeconomic interests of commercial organizations.

Ganesan and Vivekanandan (2009) described a secured hybrid architecture model for the internet banking using Hyperelliptic curve cryptosystem and MD5 is described. Information about financial institutions, their customers, and their transactions are, by necessity, extremely sensitive; thus, doing business via a public network introduces new challenges for security and trustworthiness. Given the open nature of the Internet, transaction security is likely to emerge as the biggest concern among the e-bank's account holders. The rapid growth in account hijacking and online fraud are on the rise. The negative publicity damages consumer trust in the online service. Security, which involves the use of technical advancements like cryptography, digital signature and certificates aimed at protecting users from risk of fraud, hacking or "phishing", has a positive influence on the intention to purchase online (Lian and Lin, 2008).

Indeed, in Aladwani's (2001) study of online banking, potential customers ranked Internet security and customers' privacy as the most important future challenges that banks are facing. Perceived usefulness, perceived Web security has a strong and direct effect on acceptance of internet banking, too. A high level of perceived risk is considered to be a barrier to propagation of new innovations (Ostlund, 1974). Influenced by the imagination-capturing stories of hackers, customers may fear that an unauthorized party will gain access to their online account and serious financial implications will follow.

The review of literature suggest that most of the studies have been done on issues related to Internet banking in countries like Australia (Sathye, 1999), Malaysia (Mukti, 2000; Chung and Paynter, 2002; Sohail and Shanmugham 2004), Singapore (Gerrard and Cunningham, 2003a, 2006b), Turkey vs. UK (Sayar and Wolfe, 2007) and Saudi Arabia (Sohail and Shaikh, 2007). Much work has not been done in India with regard to Internet banking issues. The present study intends to know the factors affecting the acceptance of customers and also indicates level of concern regarding security and privacy issues in Indian context.

A website discusses ATM, smart card, and biometrics technologies, with descriptions of implementation by PRODEM FFP in Bolivia, Voxiva in Peru, ICICI Bank in Asia, and BASIX in India. This report looks at the use of palm pilots and smart cards at Swayam Krishi Sangam in Andhra Pradesh [15].

In an article, Sudama project of BASIX (India), introduced, where low-interest loans are available in remote rural areas through a new computer-based transaction recording system. The new lending model supported by ICT allows a low-cost and reliable form of rural lending for microfinance [17].

VI. RESEARCH METHODOLOGY

Online banking systems require efficient security models capable of identifying users and authorizing transactions, thus mitigating fraud. However, current models are focused on fraud identification instead of fraud prevention, which means that actions are taken only after a fraud occurs instead of performing a series of preventive procedures. Analyzing the security devices implemented by the largest banks in India it is observed that several

security layers and methods are concurrently adopted [25]. Virtual keyboards are clearly one of the most used models, being adopted in different banks like State Bank of India, Punjab national Bank. However, banking 5rojans continue to successfully operate, directing security to reactive fraud identification rather than prevention. In this analysis, SSL (Secure Sockets Layer) was not considered because it is adopted in all online banking systems. Moreover, SSL only provides security from the network layer downwards but is not capable of guaranteeing protection against attacks based on the application layer, where data is captured or modified before encryption.

Basically, banking systems need to accurately identify the user and authorize his access to banking transactions. The identification schemes are based on two main factors: unique secret information previously shared by the user and the bank (such as passwords) and unique characteristics of the device which is being used to access the service (device fingerprinting).

The models currently adopted in online banking systems are based on several security layers, consisting on diverse parallel solutions and mechanisms which aim at protecting the banking application and the user's data, providing identification, authentication and authorization. These are:

Digital Certificates

Digital certificates are used to authenticate both the users and the banking system itself. This kind of authentication depends on the existence of a Public Key Infrastructure (PKI) and a Certificate Authority (CA), which represents a trusted third-party who signs the certificates attesting their validity. In Brazil, banking systems use A1 and A3 certificates issued and signed by ICP-Brasil.

One-Time Password Tokens

One-Time Password devices are commonly used as a second authentication factor, which may be requested in specific or random situations. This kind of devices render captured authentication data useless for future attacks through the use of dynamically changing passwords which can be used only once [26].

One-Time Password Cards

This constitutes a less expensive method for generating dynamic passwords, also providing a second authentication factor. However, in some banking systems, passwords generated by OTP cards are reused a number of times before being discarded, rendering this system vulnerable to short term replay attacks.

Browser Protection

In this model, the system is secured at the Internet browser level, which is used to access the banking system. The user and his browser are protected against known malware by monitoring the memory area allocated by the browser in order to detect such malware and hinder credential theft and capturing of sensitive information.

Virtual Keyboards

Virtual keyboards were developed for the efficient use of keyloggers (which capture information typed into the device). These devices are usually based on Java and software based cryptography, allowing portability between different devices. Currently they are being replaced by other more efficient methods which require less processing power and slower transmission rates.

Device Registering

This method restricts access to the banking system to previously known and registered devices. Hardware fingerprinting techniques are used in conjunction with user identification through secret credentials.

CAPTCHA

Completely Automated Public Turing test to tell Computers and Humans Apart, is a method recently adopted in some banking systems whose objective is to render automated attacks against authenticated sessions ineffective. This method requires the legitimate user to input information conveyed as scrambled images which are difficult for automated robots to process and recognize.

Short Message Service (SMS)

This method has been applied in some banking systems to notify users about transactions requiring their authorization. It provides a second authentication channel for transactions that fit certain characteristics by sending to the user a set of characters which have to inform in order to authorize and process the transaction through the online banking system.

Device Identification

Device identification is usually applied together with device registering but it is also used as a stand-alone solution in online banking systems that aim at facilitating user access. This identification model is based on physical characteristics of the user's device through which it is possible to identify its origin and history information.

Positive Identification

Positive identification is a model where the user is required to input some secret information only known to him in order to identify itself. It is applied as a second authentication method.

Pass-Phrase

It is a security model based on information held by the user. It is usually used as a second authentication method in transaction that involves money movement.

Transaction Monitoring

Even though this method is not thoroughly analyzed in the present work, it is currently applied in all online banking systems, each of them using different techniques. Artificial intelligence, transaction history analysis and other methods that identify fraud patterns in previously processed transactions are among the various approaches to transaction monitoring.

The study also employs primary data as well as secondary data. Secondary data will be collected from different published sources. Primary data will be collected by structured survey. The survey will be created online

and link sent to the respondents from India using convenience sampling.

VII. CONCLUSION

This paper will serve as an initial step in exploring customers' views and expectations on online banking. However, this paper is focused to a high degree on acceptance of online banking among Indian customers and opinion regarding security and privacy issues. Further research is required to investigate issues related to online banking in deeper manner and what strategies should be adopted by banks by which they can enhance level of e-satisfaction and e-loyalty with respect to online banking. Cloud computing is also being widely used in banking sector, and this also requires further enhancement.

REFERENCES

[1] www.banknetindia.com
[2] www.networkmagazineindia.com
[3] Catherine weir, Irain Mc Kay, Mervyn Jack, "Functionality and usability in design for e-Statements in e-Banking services", Volume 19, Issue 2, March, 2007.
[4] Lawrence F Cunningham1, James Gerlach2 and Michael D Harper, "Perceived risk and e-banking services: An analysis from the perspective of the consumer", (2005) Journal of Financial Services Marketing 10, 165–178.
[5] www.arraydev.com
[6] Nie Jin; Ma Fei-Cheng, "Network security risks in online banking", Volume 2, Issue, 23-26 Page(s): 1229 – 1234, Sept. 2005.
[7] Internet Banking 12 Comptroller"s Handbook.
[8] Comptroller's Handbook 11 Internet Banking.
[9] Comptroller's Handbook, 1999.
[10] http://rbidocs.rbi.org.in
[11] FFIEC, Information Systems Examination Handbook (IS Handbook) for a discussion of OFAC.
[12] Singal, Amit & Bikram Duggal. ICICI Bank, March 2002.
[13] Markson, T. & Hokenson, M. University of Michigan Business Case Study, December 2003.
[14] World Resources Institute, Digital Dividend. October 2004.
[15] Grameen Foundation, *Grameen Connections* 4 (2), April 2001, www.sksindia.com
[16] Gupta, S. BASIX India: Intermediate Technology Publications, June 2002.
[17] Liao, Z., & Cheung M., "Challenges to Internet E-Banking", Communications of the ACM, 46(12), 248-250, 2003.
[18] Beckett, A., Hewer, P., & Howcroft, B., "An exposition of consumer behaviour in the financial services industry". The International Journal of Bank Marketing, 18(1), 2000.
[19] Daniel, E., "Provision of electronic banking in the UK and the Republic of Ireland", International Journal of Bank Marketing, 17(2), 72-82, 1999.
[20] Mattila, M., Karjaluoto, H. and Pento, T. "Internet banking adoption among adult customers: early majority or laggards?" Journal of Services Marketing, 17 (5), 514-28, 2003.
[21] Fox, S. and Beier, J., Online banking 2006: surfing to the bank, Pew Internet & American Life Project, (2006), Banking-2006.aspx (accessed 17 March 2009).
[22] Liao, J. and Lin, T. "Effect of consumer characteristics on their acceptance of online shopping; comparisons among different product types; Computer inhuman behavior", 24 (1), 48-65, 2008.
[23] Mattila, M., Karjaluoto, H. and Pento, T. "Internet banking adoption among adult customers: early majority or laggards?" Journal of Services Marketing, 17 (5), 514-28. 2003.
[24] Liao, Z., & Cheung, M., "Challenges to Internet E-Banking", Communications of the ACM, 46(12), 248-250, 2003.
[25] Laerte Peotta, Marcelo D. Holtz, Bernardo M. David, Flavio G. Deus, Rafael Timóteo de Sousa Jr., "A formal classification of internet banking attacks and vulnerabilities", International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 1, Feb 2011.
[26] HALLER, N., A One-Time Password System (RFC 2289), Internet Engineering Task Force. [S.l.]. 1998.