IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Internet Security And Intrusion Combating In Digitalized Banking With Special Reference To Karur Vysya Bank Ltd.

Dr.K.Anjaneyulu,
Associate Professor of Commerce,
Badruka College of Commerce & Arts,
Kachiguda, Hyderabad, Telangana - 500027

Abstract

Today's banking business has taken a dramatic change in the last few years. There has become a trend and a precedent of online banking. Banks are allowing people to access anything and everything in their accounts online without ever stepping foot outside of their homes. This new age in convenience not only allows great opportunities for banks to cater to all of its consumers needs but it also allows a great opportunity for hackers to access a greater amount of information. The only way to keep ahead of the hackers is by staying ahead of them with the newest and latest in network securities and technologies. By using critical reasoning and problem
solving the banking community and its partners are better able to deal with the potential threats that lurk around every corner. Since the world of technology is always changing and the world of securities is always changing, the hackers of the world must also adapt and change to try and stay ahead of the securities industry. The network securities industry is a major business that continues to grow and thrive in a time where computer theft is increasingly present. Unfortunately, it is impossible to these companies lo catch every hacker and every criminal that enters the web. Hackers will continue to find ways to infiltrate the system just as the bank network securities will continue to find ways of keeping them out. In the end it is a split decision because even if one hacker gets into the system out of a million, the banks have still lost a battle in ever continuing war.

Key words: Internet Security, Intrusion Combating, Virtual Bank, Credit Union.

1. Introduction

Internet banking allows customers to conduct financial transactions on a secure website operated by their retail or virtual bank, credit union or building society. E-banking solutions have many features and capabilities in common, but traditionally also have some that are application specific.

The common features fall broadly into several categories like:

A. Transactional (e.g., performing a financial transaction such as an account-to-account transfer, paying a bill, wire transfer, apply for a loan, new account, etc.)

(i) Payments to third parties, including bill payments and telegraphic/wire transfers.
(ii) Funds transfers between a customer's own transactional account and savings accounts.
(iii) Investment purchase or sale.

(iv) Loan applications and transactions, such as repayments of enrollments.

B. Non-transactional (e.g., online statements, cheque links, cobrowsing, chat).
(i) Viewing recent transactions.
(ii) Downloading bank statements, for example in PDF format.
(iii) Viewing images of paid cheques.

C. Financial Institution Administration.

D. Management of multiple users having varying levels of authority.

E. Transaction approval process.

F. Features commonly unique to Internet banking include personal financial management support, such as importing data into personal accounting software. Some online banking platforms support account aggregation to allow the customers to monitor all of their accounts in one place whether they are with their main bank or with other institutions.

The Indian Banking landscape has witnessed a sea change in the area of delivery of services on account of technology initiatives during the last few years and this has enabled the customers to complete majority of their banking transactions remotely through alternate delivery channels. ATM proved one of the successful channel banking and helped the customers to avail some of the banking facilities round the clock throughout the year. Though, it is a value addition, still customers need to pay a visit ATM, which involves sparing of scarce resources such as time and money. Today's discerning customers are looking beyond Branch and ATM and would like to attend their banking requirements as per their convenience either through Home/Office or while on travel. Thus, the introduction of Internet banking has provided the facility of banking from home/office without physical intervention of the branch or ATM.

Review of Literature

1. Arunangshu in his paper focused on digitalization of the rural banking system in India. Digital banking systems have enormous potential to change the landscape of financial inclusion. They found that with the features of low cost, ease of use of digital banking can accelerate the integration of the unbanked economy to the maintenance.

2. Rajeshwari in her research paper found that digital banking increases the expectations of customers Hom banks. With the help of secondary data, they analyze that digital banking has become the milestone in the Indian banking system. It enhances the growth and progress of Indian banking. It found that due to digital banking the operating cost of banks has been reduced rapidly. Lower operating cost means more profits for the banks. According to him, digital banking has the power to change the banking structure.

3. Aarti Sharma, in her research paper concluded that digital banking will prove a milestone in the Indian economy. The study is analytical in nature and based on secondary data. According to her, digital banking impacts the Indian economy. With the change in the technology of the banking system, the economy also faces the changes. It can provide better services to their customers. Due to their rapid growth, it is acceptable in the market. Now by analyzing the benefits of digital banking everyone in the market demanded this for the overall growth and success.

4. Kiran Jindal conducted research and analyze that with the promotion of digital banking it is also necessary to enhance awareness and preference of customers for banking products. It basically emphasis on HDFC banking products. The paper is based on empirical study. They can use primary data for the study. With the use of questionnaire, they collect the data they analyze that age factor is most effective factors which effects the digital banking system. The customers over the age of 35 doesn't accept the change and still they are dependent upon public sector banks other than private sector banks. Customers are not much aware of the new technology. So, it is very important for the success of digital banking is to promote awareness among customers.
For analyzing the data researcher use SPSS software.

5. Ruby in her paper studied the problems and prospects of E- Banking. It also focuses on the pros and cons of digital banking which affects the customers' Perceptions. They also focus on the risk involved while introducing digitalization in the market. The secondary data was used for the research paper. They concluded that E- Banking offered a high level of convenience for managing finance for the customer in the digital market. They also analyzed the risk means financial security, personal privacy towards the customers

6. Vishal conducted a study and concluded that customers always want safety and security during cash transactions. This Paper makes more emphasis on the perception and opinion of urban mobile banking users. He focuses on practices, challenges and security issues related to mobile banking in India. He uses a quota sampling method. The data is collected from the primary source of data. The sample size is 100 respondents divided into two categories: 50 users and 50 non- users of mobile banking. The sample is taken from Ghaziabad city. It was analyzed that knowledge regarding use of mobile phones was the most important issue in mobile banking due to availability of various handsets models supporting different types of technology in the market. Chandrawati identified the drivers of digital banking transformation for the Indian banking system. E-Technology has become a tool that facilitates banks" organizational structures, business strategies. customer services and related functions. Using exploratory research, the study concluded that digitization changed the face of branch banking and mobile was being increasingly used as a primary channel of banking. Moreover, integration with social media components as their online channels was also a major driver for digital banking transformation

7. Sahu and Kumar studied the important factors responsible for successful implementation of the digital payment (e-Payment) system in India. Conducting a qualitative study with extensive literature review and using interview and expert opinion, 13 success factors namely Anonymity, Bank Involvement, Drawer, Infrastructure, Mobility, Parties, Popularity, Range of Payment, Risk, Security, Transfer limit, Transfer mode, and Transfer time were responsible for successful implementation of digital payment at Allahabad city.

8. Ankit and Singh conducted a study to analyze the impact of technology acceptance model (TAM) in the context of internet banking adoption in India under security and privacy threat. Keeping the TAM proposed by Davis as a theoretical basis, the paper revealed that perceived risk had a negative impact on behavioral intention of internet banking adoption and trust had a negative impact on perceived risk. A well-designed web site was also found to be helpful in facilitating easier use and also minimizing perceived risk concerns regarding internet banking usage.

Objective of the Paper

The basic aim of the paper is to identify and evaluate the internet Security Issues in Digitalized Banking Arena with a focus on how to combat the intrusion related problems. However, the paper is guided by the following sub objectives:

(i) To identify the key concerns of Network Security in digital banking
(ii) To explore the best practices in Internet Banking at Karur Vysya Bank Limited and
(iii) To know about the steps to be taken care while operating Internet Banking to avoid frauds.

2. Key Concerns of Network Security in Banking System

i) Confidentiality

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network.

ii) Integrity

In information security, integrity means that data cannot be modified undetectably. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

iii) Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

iv) Authenticity

In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.

V) Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. Electronic uses technology such as digital signatures and public key encryption to establish authenticity and non-repudiation.

3. Security Attacks and Intrusion in Banking

i) As shown in the Figure 1, Most of the attacks on online banking used today are based on deceiving the user to steal login data and valid TANs. Two well-known examples for those attacks are phishing and pharming. Cross-site scripting and key logger/Trojan horses can also be used to steal login information.

ii) A method to attack signature based online banking methods is to manipulate the used software in a way, that correct transactions are shown on the screen and faked transactions are signed in the background.

iii) A recent FDIC Technology Incident Report, compiled from suspicious activity reports banks file quarterly, lists 536 cases of computer intrusion, with an average loss per incident of $80,000 at the end of the Financial Year 2015.

iv) The most recent kind of attack is the so-called Man in the Browser attack, where a Trojan horse permits a remote attacker to modify the destination account number and also the amount.

v) Digital Thieves

Bank network security is an imperative part of the banking industry because there are always people trying to gain some type of access to the infrastructure of a bank. In today's new age of technology, the "bank robbers" of times gone by is no longer the same type of criminal that we see. Today's society is more susceptible to crime and infiltrations than ever before in history. The most disheartening aspect of a lack of security is that a bank could be hacked and robbed without ever knowing who it was or were it was being done from.

1. Security Measures Practiced by Financial Institutions

(i) Security Token Devices

Protection through single password authentication, as is the case in most secure Internet shopping sites, is not considered secure enough for personal online banking applications in some countries. Basically, there exist two different security methods for online banking. The PIN/TAN system where the PIN represents a password, used for the login and TANs representing one-time passwords to authenticate transactions. TANs can be distributed in different ways; the most Popular one is to send a list of TANs to the online banking user by postal letter. The most secure way of using TANs is to generate them by need using a security token. These token generated TANs depend on the time and a unique secret, stored in the security token (two-factor authentication or 2FA). The SMS text usually quotes the transaction amount and details; the TAN is only valid for a short period of time. Especially in Germany, Austria and The Netherlands, many banks have adopted this "SMS TAN" service as it is considered very secure. Signature based online banking where all transactions are signed and encrypted digitally. The Keys for the signature generation and encryption can be stored on smartcards or any memory medium, depending on the concrete implementation.

(ii) New Technology

Today's banking business has taken a dramatic change in the last few years. There has become a trend and a precedent of online banking. Banks are allowing people to access anything and everything in their accounts online without ever stepping foot outside of their homes. This new age in convenience not only allows great opportunities for banks to cater to all of its consumers needs but it also allows a great opportunity for hackers to access a greater amount of information. The only way to keep ahead of the hackers is by staying ahead of them with the newest and latest in network securities and technologies. By using critical reasoning and problem solving the banking community and its partners are better able to deal with the potential threats that lurk around every corner. Since the world of technology is always changing and the world of securities is always changing, the hackers of the world must also adapt and change to try and stay ahead of the securities industry. Who will win the battle of man vs. computer? The network securities industry is a major business that continues to grow and thrive in a time where computer theft is increasingly present. Unfortunately, it is impossible to these companies to catch every hacker and every criminal that enters the web. Hackers will continue to find ways to infiltrate the system just as the bank network securities will continue to find ways of keeping them out. In the end it is a split decision because even if one hacker gets into the system out of a million, the banks have still lost a battle in ever continuing war. Firewalls can also be configured to block everything except specified traffic. Unfortunately, Internet attackers can easily circumvent firewall blocking techniques. FTP servers can use a different port. and websites can act as gateways to blocked sites without your fire wall knowing.

(iii) Intrusion Detection

The second Pillar of network security is Intrusion Detection Systems (IDS). These systems look for intrusions in process such as accessing a forbidden website' or 'Trojan horse attempting to control a workstation,' The IDS records each dangerous pattern and alerts network security Personnel. This approach is highly effective in discovering illicit traffic. However, IDS must be
carefully configured to send alerts only on dangerous traffic. A mistuned IDS often sends alerts on Perfectly normal traffic, and may miss dangerous packets because it isn't looking for them. Also, the IDS is unable to stop troublesome network traffic. Someone must review the attack information and attempt to block it. This can take time, and sometimes cannot be completed before the network sustains lasting damage.

(iv) Intrusion-Prevention-System

Intrusion-Prevention-System (IPS) combines the firewall and IDS technologies. IPS watches network traffic like IDS and determines whether to pass any given traffic like a firewall.

The IPS actually assesses traffic patterns to evaluate the type of network access and to determine.
Whether it should be permitted. While IDS can only note an ongoing attack and pass the alert to an analyst, the IPS will stop the attack by blocking traffic between the attacker and its victim. Careful configuration is very important for the IPS. Mis-configured IDS will only send harmless alerts which can be ignored; but a mis-configured IPS will deny legitimate traffic, giving network staff and employees huge headaches when they become victims of mistaken digital identity. However, when properly tuned, an IPS is an incomparable defense against network-based-attacks.

(iv) A Bank's Network Defense Strategy

Could your bank forego firewall and IDS devices in favor of an IPS? Possibly. But COCC finds that well-defended banks typically install all three pillars of security when they construct their
network defenses. We recommend that traffic arriving at the bank’s network first pass through an
IPS that watches for abnormal service requests and automatically denies anything resembling an
Internet- based attack. Your bank can work with its IPS vendor to minimize disruptions of legitimate network traffic. Once past the IPS, your Internet traffic encounters the firewall. We set these devices to deny nearly all incoming traffic except for replies to outgoing requests and a limited selection of services such as website traffic and incoming email. Finally, from within the bank's network, we recommend a large network of IDS sensors to monitor the network for anomalous traffic. This final line of defense alerts bank staff to unusual traffic patterns and then determines whether further action is needed.

INTERNET BANKING AT KARUR VYSYA BANK LTD.:

Internet banking is a system allowing individuals to perform banking activities at home, via the Internet.

For the past few years, banks are focusing attention on Internet banking through offering variety of services such as balance enquiries, transfer of funds between accounts and make requests for cheque books as well as opening of accounts, opening of fixed deposits, donate online round the clock.

About Karur Vysya Bank:

KVB rated as the Best mid-sized bank by business today, is a leading financial institution established in the year 1916. KVB continues its endeavors to bring the best of products and services to its customers to emerge as the techie bank that provides the gateway to smart way to bank. All the branches of KVB are powered with Core banking solution CBS. KVB has its own portal: karur vysya bank (KVB) Internet banking, through which it offers

different online services for the customers. The KVB internet banking is a free service available to all its customers 24X7, allowing them to access their accounts any timer across the globe.

The services offered at KVB Net banking are : Account details, Online account statements, transfer of fund online, online details, contact customer service, fast and safe payment options for travel and ticket reservations, phone bill payments, cable, DTH, internet service providers etc..

Applications of Internet banking at KVB:

The customer can have the following facilities while operating the Internet banking at KVB

* My Accounts
* Transfer funds
* Loans
* Customer Services

(i) My Accounts:

Customers can have the details of all the current and savings accounts mapped the specific customer ID. Details including the account number, name of the account, and the current balance of all the CASA (Current accounts and savings accounts) accounts mapped to the customer ID can be viewed.

(ii) Transfer Funds

Customers can transfer funds without any time restrictions from any of the accounts to any other account with in KVB as well to accounts with other banks through RTGS (Real Time Gross Settlement).

(iii) Loans

All corporate loan accounts can be mapped to a particular customer ID. Specific detail such as the Loan due date, the next installment due date, Letter of Credit, Export and Import bills, etc can be viewed.

(iv) Fixed Deposits

Customers can open the fixed deposits for various periods through Net banking and the same will be credited to the account after maturity.

(v) Customer service

(vi) Customers can view the status of a number of services like:

* Cheque status· To Know if a particular cheque is paid or not.
* Stop cheque payment - To stop the payment of the cheque.
* Forex rate enquiry.
* Mail Box.
* Cheque book status enquiry.
* Registering alerts- To register for alerts and messages.
* Session summary report- To know the summary of the log-in activities.

(vii) Other services

KVB also offers various other facilities such as utility bill payments like electricity bill, Telephone bill, Cable bill, Payment of Mutual funds, Insurance, Credit card bill payment, online

shopping. Air and Train Ticket booking, Internet bill payment, donate online, apply for a loan etc.,

Steps for safe and secure Internet Banking:

* Internet Banking should be accessed from Personal or office computers only, Cyber cafes should be avoided.

* Never reply to emails asking for password or pin.

* Verify the domain name displayed on the site to avoid spoof websites.

* Identity then is a real and growing problem today. Be protective of the personal account information whenever doing transactions online.

* Routinely check the computer for spy ware and viruses and update the anti-virus software.

* Do not reveal or share your banking information or online banking/payment card user-ids and Passwords to any third party.

* Verify that the banking portal has high-end encryption software in place.

* KVB also provides various other secured facilities while operating Internet banking to avoid frauds and to provide a better banking experience to its customers.

* KVB protects all the online banking activities and information of its customers. It also uses an extra layered security methods providing the customer with an additional feature called RSA Token which is required to provide the information while doing online fund transfer.

* The six-digit secret number of the RSA Token changes for every 60 seconds which reduces the chances of fraudulent online Transactions.

Conclusion

Online banking is exploding worldwide and expected to grow to nearly 900 million users by 2015. Financial institutions are responding to the demands of their customers for the convenience of their customers. Despite the convenience offered to end users, online banking is vulnerable to a myriad of threats. By using critical reasoning and problem-solving the banking community and its partners are better able to deal with the potential threats that prowl around every corner. The technological development induced in the world has slowly developed plenty of software packages and systems eventually to address the potential intrusion in to financial institutions data bases.

This study provides various benefits of Internet banking offered by Karur vysya bank which creates a better banking experience for its customers. lt also provides the tips to be followed for safe and secure Internet banking. In true Internet banking, any inquiry or transaction is processed online without any reference to the branch at any time. Providing Internet banking is increasingly becoming a "need to have" than a "nice to have" service in the present-day banking.

References

1. William Stallings "Cryptography and Network Security", Third edition.

2. R.K. Uppal and Rimpi Jatana "E-banking in India - Challenges and Opportunities".

3. Mahmood Shah, Steve Clarke "E-Banking Management: Issues, Solutions, and Strategies"

4. Denek Atkins "Internet Security Professional Reference".

5. Bruce Schneier "Applied Cryptography".

6. Sharma Aarti, “Digital Banking in India: A review of Trends, Opportunities and Challenges”, IRJMST, vol.8, issue 1,PP.1680180.

7. Aladwani A.M, “Online Banking: A Field study of drivers, development, challenges and expectations”, International Journal of Information Management, vol. 21, pp. 213-225.

8. Rajeshwari M, “Digital Banking and Indian Perspective”, International Journal of Economics and Finance, Vol. 10, issue 3, pp. 1-5.

9. Jindal Kiran, “Customer Awareness and Preference for Digital Banking offered by HDFC Bank: An Empirical Study”, Journal of Internet Banking and Commerce.