www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 4 April 2017, Page No. 21051-21060
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i4.43

Internet Banking System & Security Analysis

Rahul Kumar, Dr. Abhineet Anand
Email id:-rahulkumarisro@gmail.com
School of computing science and engineering
Galgotias university

Abstract:

Internet banking or E-banking has attracted the attention of banks, securities, insurance companies in developing nations since the late 1990s and the rapid and significant growth in electronic sectors and commerce it's obvious that electronic (online internet) banking and payments are likely to advance or rapidly increased.

Introduction:-

Major Challenges For E-Banking In India: - E-Banking in India is its emerging state of development. Most of them are basic services only the deregulation of e-banking industry coupled with the emergence of new banking technology is enabling new competitors to enter the financial services to enter the financial services markets quickly and efficiently. However, it needs to be recognised that perception norms and an improvement in the functioning of services.

Acceptance Of Customers: - Proper understanding of the customer is the major aspect of the E-Banking.It knows that computer literacy in India is yet very low and is problems in fast acceptance of the internet. Altitude of the Indian customers needs to be changed by giving by awareness technical terms in Internet Banking.

Costly Technology: - It connects with Start up cost e-banking is huge at initial level for acquiring personal computer and other equipments, oneself to do online banking is still not with in the reach of the middle class and upper-middle class customers.

Issues In Security: - In a paper less transactions, many people of security are involved. A secrecy threat as circumstensive decision to cause the economic hardships to data, and construction of network resources, disclosure, modification of data or fraud, denial in services and distortion of information. Providing appropriate security of using encryption techniques, implementation of firewalls and virus protection spyware etc.

LEGALISSUES: -In today's banking world, the legal framework for recognising the validity of banking transactions, conducted through the internet is still being put in place. Information technology act provides security & legal framework for e-commerce transactions as well as e-banking. Information technology act provides security & legal framework for e-commerce transactions.

How Can We Deal With It: -People should be made aware and trained regarding e-banking to the people in their various institutions so that people can become friendly to e-bank.

DOI: 10.18535/ijecs/v6i4.43

E-Banking will pave way for cashless economy, which will bring transparency into the system as it is in Sweden. Sweden is the only cashless country in the world. Almost all the transactions are carried out through the plastic currency that has reduced to the tremendous reduction in corruption and black money.

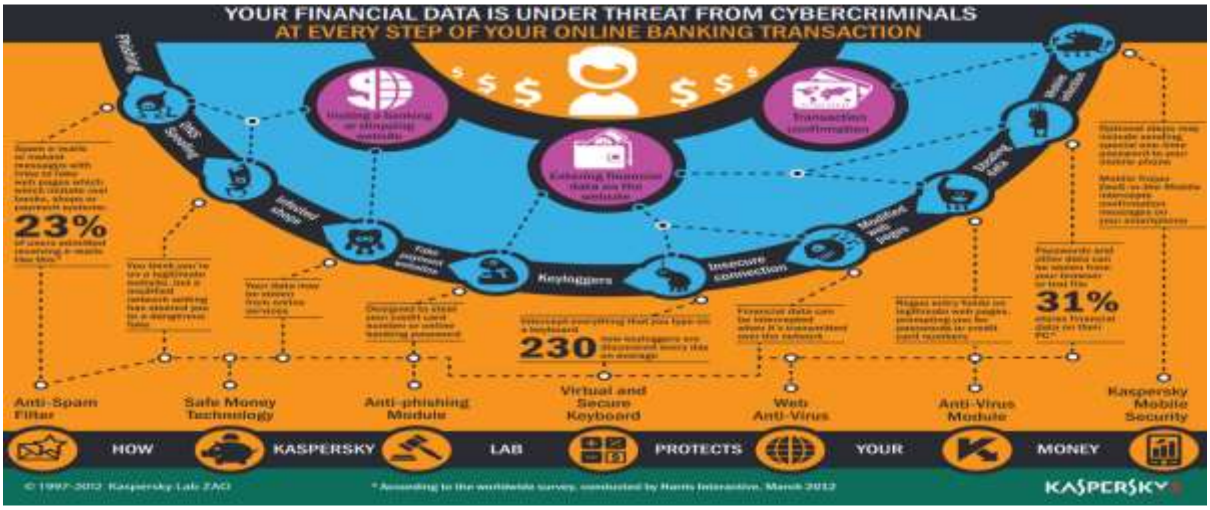
Recently govt demonetized 1000 and 500 currency notes, that is causing problem to people as they have to stand in long queue to get the cash, we have seen that most of the people are using paytm and other such applications for various transactions, so this is the best example how e-banking can reduce problems. SO, the point is that more and more private companies should come up with such applications to promote e-banking.

EXPENSES: -The major problem that comes up is the expenses, so to meet this problem, govt should come up various schemes like Digital India that has been launched recently, besides that a fund should be released separately for such schemes. The government should release the tender for IT companies that are interested in investing in such sector.

Security Issue: - One of the major factors in e-banking is about its security features, recently, we have seen that data of around 65 lakhs debit card was stolen. SBI, HDFC, YES and various other banks were the victim of it, as a malware software was released through Hitachi Payment Agency, that lead to stealing of data. This incident shocked the nation and people started doubting the e-banking system. So, a major responsibility of such companies and banks is to provide security to their customers, so that they can confidently go for e-banking, without any fear of losing their data.

Cyber Security In Internet Banking:-

1. Introduction: -E-banking is an attractive target for attackers and the easiest way of stolen (stealing) money in e-banking is to attack its weakest point are the client.In brief, ideas how to attack client authentication and transaction authorization and processes.


YOUR FINANCIAL DATA IS UNDER THREAT FROM CYBERCRIMINALS
AT EVERY STEP OF YOUR ONLINE BANKING TRANSACTION
Phishing
DNS Spoofing
Infected shops
Fake payment websites
Keyloggers
Insecure connection
Modified web pages
Stealing data
Mobile malware
Transaction confirmation
Entering financial data on the website
23%
31%
230
Anti-Spam Filter
Safe Money Technology
Anti-phishing Module
Virtual and Secure Keyboard
Web Anti-Virus
Anti-Virus Module
Kaspersky Mobile Security
HOW KASPERSKY LAB PROTECTS YOUR MONEY
© 1997-2012 Kaspersky Lab ZAO
KASPERSKY

This above report are generated by Kaspersky lab(Antivirus)

2. Overview

We assume that the attackers know the client's username and their password for their e-banking system. If there was no extra secret used to perform a transaction, the attackers could take a full control of the client's account and be minimize the risk of stealing the client's money and two security layers are used.

1) The client has to authenticate. If it is done successfully and the clients can only view their account. When the clients wants to perform a transaction and he needs to deliver another secret the authorization password. The attackers want to get very high returns on their investment. He needs something scalable to reach this goal or main purpose. Phishing and malware are two things to seem to be a good choice for both client's authentications and transaction authorizations.
2) Phishing (same pages) can be automated when sent via email. Some people are not aware of the risk. Malicious code can be included in an interesting game available for free. People download and install the game together with malware. The game looks fine and people aren't aware of the risk and they connect later to internet banking system and finally this is what the attackers is waiting for this situation.These are the only examples but they show how a typical e-banking client's that is unaware of the risk, and can be attacked.One may say that there are malware and phishing detection mechanisms that will stop the attackers and the problem is that they detect known attacks and try to detect unknown attacks. That is why there is no surety to detect the attacks.

3. Client authentication

When the client wants to get access to the e-banking system, he needs to first authenticate. He connects to a bank via SSL or TLS and gets a digital certificate. The browser does not display a warning when the certificate is digitally signed by one of the trusted Certificate Authorities (CAs). The client typically enters his username and password to log in to internet banking system and before it happens, the client should check whether the certificate belongs to the bank he wants to communicate with.

Now analyse how phishing and malware can be used to steal the client's securities.

3.1 Phishing

Not everyone understands how certificates work. Then, it might be enough to send the clients a link to a domain not protected by SSL/TLS that looks similar to the legitimate one. Some clients will not notice the difference. If they click the link, the attacker will be able to collect their information regarding their accounts.

Let us assume that the client always checks whether SSL/TLS is used when communicating with the bank. The attacker might have received a digital certificate signed by one of the trusted CAs for the domain and that looks similar to the one. Then the client can see that SSL/TLS is used when he connects to the bank and the browser does not display a warning. When the client does not check who the owner of the certificate is and he might reveal the credentials to the attackers.

Masked or complicated password are sometimes used when the clients are authenticating. The clients are asked to enter selected password. Thus, the attacker needs more attempts to get the entire password, but it does not have to be a problem for him. The attackers can ask the clients to enter the entire password. Some of the peoples will probably do what the attackers want.

The bank might also share a picture with the client. When the client gets authenticated, he can see this picture. Then the client knows that he is communicating with a bank – the attacker doesn't know the picture. This way, successful phishing attempts can be detected as long as the client always verifies that the picture appears when he becomes authenticated. When the picture doesn't appear, the client knows that something is wrong. He should then connect to the legitimate e-banking system immediately and change the password.

3.2 Malware

In this section that the client's machine got infected.

It does not help when the client knows how certificates work. Everything is fine from the client's point of view - the bank's certificate is digitally signed by one of the trusted CAs and the client checks that it belongs to the bank he wants to communicate with. But the malware is able to learn the password when it is being entered on the website.

Shared pictures between the bank and the client also do not help. The client logs in and the picture appears. The client isn't aware that the malware learned the password when he was authenticating.

Masked passwords also aren't a problem for malware – it can silently analyze subsequent log-in attempts to learn the entire password.

The on-screen keyboard is sometimes used to prevent keystroke logging. But it does not prevent the malware from learning the client's password – the malware is able to capture screenshots with mouse positions.

4. Transaction authorization

Let us analyze how phishing and malware can be used to steal the authorization passwords.

4.1 Phishing

Let us assume that the client has a list of printed one-time passwords (OTPs). He is asked to enter the password from the list to authorize the transaction. When the password has already been used, it is useless for the attacker. That's why it is better than a static password but doesn't stop the attacker. The OTPs are not related with the transaction details. That's why the attacker can use phishing techniques to get several OTPs and perform arbitrary transactions. When phishing is used, the client might be informed that the bank introduced new security mechanism and the client is required to prove his identity – he is asked to enter, for example, three OTPs. Some people will probably do what the attacker wants – from their point of view the bank improves security.

A token can also be used to generate the OTPs. It could have a clock synchronized with the authorization server and share a secret with the server. The token is used to create authorization passwords valid for a certain time, for example, 60 seconds. This is better than the list of one-time passwords because when the attacker gets this password, he can use it only within a short period of time. In addition, the attacker can't perform multiple transactions if there is only one transaction allowed in this time range. But the problem is still the OTP not related with transaction details – phishing is possible.

4.2 Malware

It's assumed in this section that the client's machine got infected.

The client wants to perform a transaction. He enters transaction details and is asked to provide the authorization password. Let's assume that the password is not related to transaction details (for example, the OTP is generated by a token). The client enters the password and authorizes the transaction. But before it is sent to the bank, the attacker changes the data; for example, the destination account. This is the man-in-the-browser attack (MITB).

Let's assume, that the client enters the transaction details and is asked to provide the authorization password that is related to the transaction. The authorization password is sent by the bank to the client's machine, together with the transaction details. When this is a case, the MITB attack can still be used to change the destination account. The attacker knows what transaction the client wants to perform and displays the transaction details expected by the client instead of the ones received from the bank. From the client's point of view, everything is fine – he authorizes the transaction.

Let's discuss this case; when the client's machine is used to access an e-banking system and a mobile device is used for transaction verification (An SMS is sent to the client's mobile with the transaction details and the authorization password). Now the client can verify the transaction even if his machine is compromised. It works fine as long as the attacker doesn't infect the client's phone. Let's assume, that the client logs into the bank account. Then the malware can display the message that the bank introduced new security mechanisms

– the client has to download the certificate to his mobile phone. Everything looks fine for the client. He is asked to enter the phone number. The client gets the SMS message with a link to a certificate (this is in fact malware). It is downloaded and installed by the client. Now the client's computer and mobile are controlled by the attacker. The client wants to transfer money. He enters the transaction details and the MITB attack changes the destination account. The authorization password is sent to the client's mobile with the transaction details. The SMS brings the destination account of the attacker, but the attacker can change it because he controls the mobile and knows what transaction the client wants to authorize.. From the point of view of the client, everything is fine. The client again authorizes the transaction.

The client can also use modern mobile apps to get an access to e-banking and perform transaction verification. Then it is enough to compromise the mobile.

5. Conclusions

Two security layers are introduced to reduce the risk of stealing client's money – client authentication and transaction authorization. When the attacker gets the client's credentials, he needs another secret to steal the client's money – the authorization password.

Authorization passwords should be related with transaction details. When this is the case, the attacker can't perform an arbitrary transaction if he gets the authorization password. Then phishing is useless for the attacker. The problem is still malware, when the client's machine used for transaction verification, is still compromised. At the first glance, modern smartphones seem to be a good choice for transaction verification – they are ubiquitous and no extra device is needed for this purpose. But they are multifunctional devices and have the same security problems as personal computers. That's why it's proposed to use a dedicated device for transaction verification.

A dedicated device could share a secret with the bank and require the client to enter the transaction details. Then it generates the authorization password. This is the only action the dedicated device does – network connectivity, for example, is not needed. Thus, the security is improved as a consequence of complexity reduction. Finally, the client enters the password on the website to authorize the transaction. It allows the bank to detect MITB attacks provided that the dedicated device is not compromised. There is a usability problem, however. The client has to enter the transaction details twice (the website and the dedicated device).

The solution might be a dedicated device with a built-in camera that is used to take a picture of the Quick Response (QR) code displayed by the bank. The code includes encrypted transaction details sent by the client and the authorization password related with this transaction. The encryption key is shared by the bank and the dedicated device. That's why the client can verify the transaction details without entering them on the dedicated device. Moreover, he can extract the authorization password that is entered on the website to authorize the transaction.

Benefits with Security:-

Payments and transfer: -Managing your money is easy. Pay your bills or transfer money in the UK or abroad.

- Immediate access 24/7: -Internet Banking gives you the flexibility to manage your money at any time, 24/7, 365 days a year.
- Safe and secure : - We take security very seriously and do all we can to keep our customers secure.
- Fast track your applications: -Applying for products through the Internet Bank is quicker because we know you.

You can also enjoy with internet banking……

- Access your balance, available balance and statement history any time.
- Manage your credit card.
- Set up regular payments and view Direct Debits.
- Get an instant response to overdraft requests (subject to approval).
- Keep track of your loan or mortgage account.

What to expect:-

Here are some of the features available through online banking:

- **View balances:** Checking your balance doesn't require much work. You simply select Account balances and take a look at your balance and past transactions. If you have more than one account, you can also do transfers between accounts.

- **Pay bills**: To pay your bills online, you just need to add to your account the names of the companies you wish to pay bills to. In the Pay Bills section, select Add payees, search for the name of the company and fill in the account number for each company. You can also sign up for the ebills service from epost, a service that sends you a bill by email instead of a printed one by regular mail.

- **Transfer funds:** When you select Transfer Funds, you'll be asked where to transfer the money to and from, when, and the amount.

- **Set up recurring bill payments or transfers**: If you make a regular payment every month, it might be convenient to set up an automatic withdrawal from your account.

- **Monitor CIBC investments**: If you have any CIBC investments, you can keep an eye on those stocks or mutual funds here.

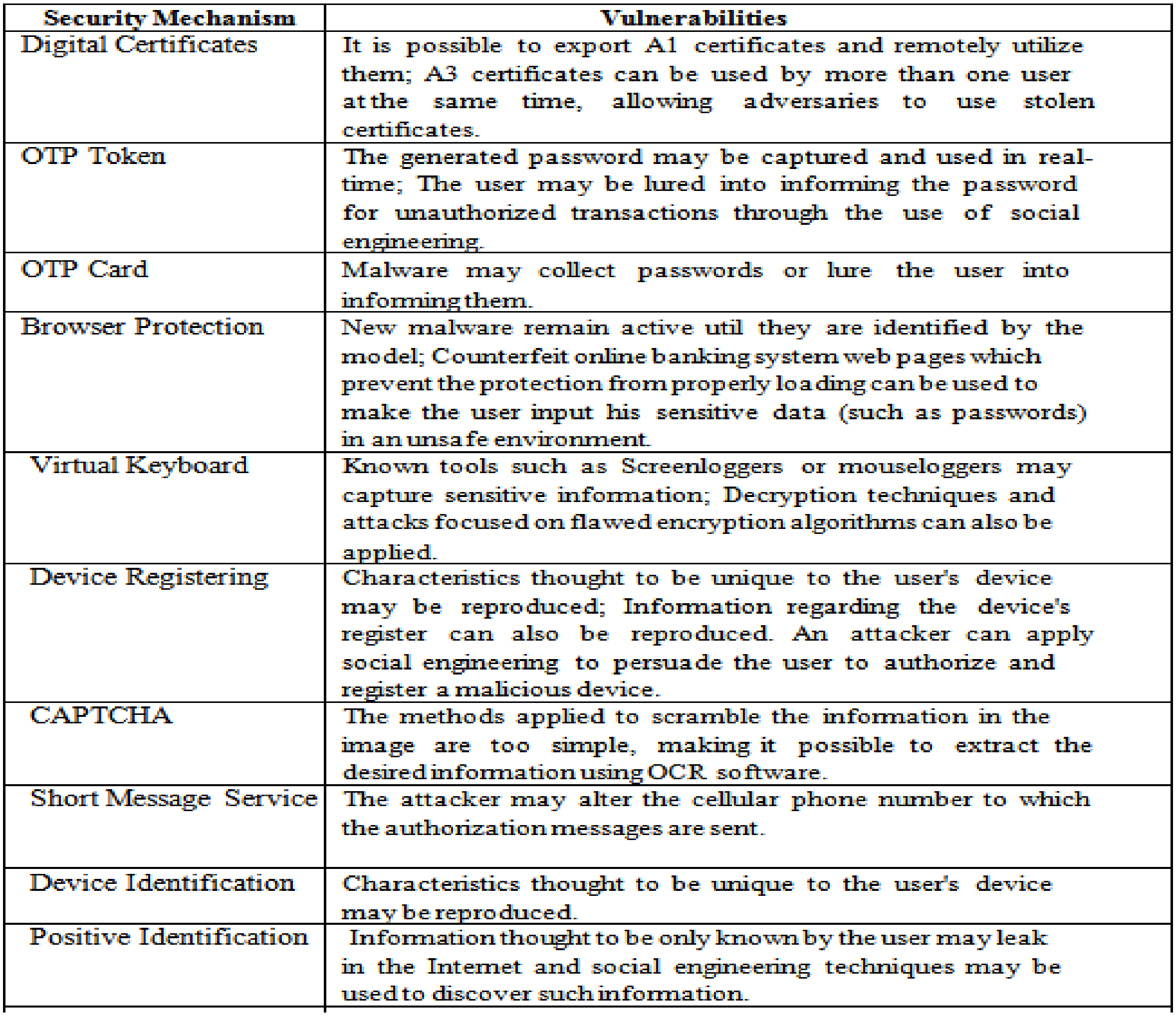
- **Send and receive an INTERAC e-TransferTM2:** This could be the end of the birthday cheque! You can receive transfers from other people's accounts, or set up transfers from your account to someone else's. The recipient will get an e-mail notifying them of the transaction.

- **View CIBC VISA* accounts:** Always a good place to monitor your spending. You can make your credit card payments online, right from your account.

- **Order cheques**: We don't need them much anymore due to online banking and debit purchases, but if you still use cheques, you can order them directly from the CIBC website.

Vulnerabilities in the online banking system:-

Table 1 presents known vulnerabilities which affect each security mechanism developed by various organisations. The correct identification of the threats faced by the current Internet Banking Systems is essential for designing more efficient models which provide the higher level of security.



Security Mechanism	Vulnerabilities
Digital Certificates	It is possible to export A1 certificates and remotely utilize them; A3 certificates can be used by more than one user at the same time, allowing adversaries to use stolen certificates.
OTP Token	The generated password may be captured and used in real-time; The user may be lured into informing the password for unauthorized transactions through the use of social engineering.
OTP Card	Malware may collect passwords or lure the user into informing them.
Browser Protection	New malware remain active util they are identified by the model; Counterfeit online banking system web pages which prevent the protection from properly loading can be used to make the user input his sensitive data (such as passwords) in an unsafe environment.
Virtual Keyboard	Known tools such as Screenloggers or mouseloggers may capture sensitive information; Decryption techniques and attacks focused on flawed encryption algorithms can also be applied.
Device Registering	Characteristics thought to be unique to the user's device may be reproduced; Information regarding the device's register can also be reproduced. An attacker can apply social engineering to persuade the user to authorize and register a malicious device.
CAPTCHA	The methods applied to scramble the information in the image are too simple, making it possible to extract the desired information using OCR software.
Short Message Service	The attacker may alter the cellular phone number to which the authorization messages are sent.
Device Identification	Characteristics thought to be unique to the user's device may be reproduced.
Positive Identification	Information thought to be only known by the user may leak in the Internet and social engineering techniques may be used to discover such information.

Easy Accesebility: - E-Banking Agencies should set up their branch office in almost every district so that people approach them easily if they meet any problem.

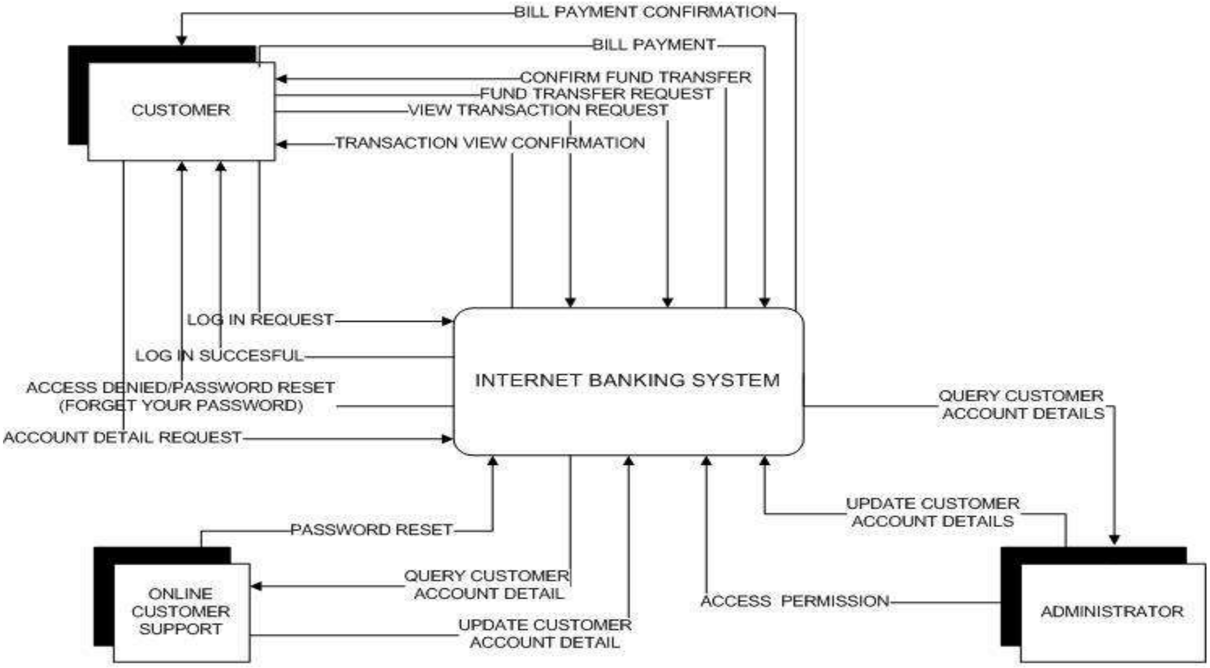
Pros and Cons of Internet Banking System:-

1) The prominent point of Internet banking is that it is very convenient for customers rather than traditional banking system and can available 24/7 and time saving.

2) Customer can access their account anytime and anywhere no need to go the bank.

3) Customer can also check their account information and also make funds transfer to their payee.

4) The customer can update their profile such as changing their address, their phone number and so on and it can be very easily.



CONTEXT DIAGRAM :
INTERNET BANKING SYSTEM

1) Gender Wise Usages Of The Internet Banking

Frequency of Use (Times per Month)	Percentage of Total Respondents		
	Female	Male	Total
Never	-	-	1.0%
1-5	15.8%	40.7%	56.5%
6-10	9.3%	22.2%	31.5%
10-15	3.7%	1.9%	5.6%
16-20	-	2.7%	2.7%
Above 20	-	2.7%	2.7%

In the tabular form data which are based on Gender Wise Usages of the Internet banking in which we can analyzed that a significant proportion of Internet banking users (56.5%) use Internet banking 1-5 times a month, which is low compared to the e-developed countries, and also Asian counterparts like Korea and Japan. Another 31.5% are using e-banking 6-10 a month.

Gender wise usage of the Internet banking reflects a polarization towards males.

2) E-Banking Services Of Foreign Banks

Banks	Daily Transactions	Account Information	Transfers	Other
	Percentage of Respondents			
ABN Amro Bank	100%	100%	30%	30%
Bank of Punjab	60%	80%	0%	20%
Canara Bank	100%	100%	0%	0%
Citi Bank	100%	83%	50%	33%
HDFC Bank	62%	85%	50%	33%
HSBC	100%	0%	0%	0%
ICICI Bank	75%	83%	8%	13%
IDBI Bank	86%	0%	0%	0%
State Bank of India	100%	33%	0%	0%
Standard Chartered Bank	100%	0%	50%	0%
UTI Bank	86%	100%	14%	0%

Here we can analyze that there are many foreign banks which are provide E-BANKING SERVICES. In this form of data, reveals that the E-BANKING SERVICES of foreign banks and some flag public sector banks are used primarily for daily transactions and private banks like HDFC, BOP ICICI are lagging. Similar results are also shown above.

Citibank and ABN Amro bank are popular among their customers for Internet Banking. In general, people are highly concerned about security and therefore they do not rely on the public sector banks for Internet fund transfers.

Conclusions :-

After all, in this era where technology is changing day by day, we need to switch from traditional methods to the smart method. Today, e-banking is emerging as a very effective technical tool is every aspect whether its corporate sector, government sector or in daily use transactions. E-Banking will not only reduce hardships but will also help to kerb black money and corruption as we have seen in the case of Sweden. Today, we need to be more friendly with e-banking, we know that achieving cashless economy at present, promotion of e-banking, especially in rural areas is very important.

Acknowledgments

I especially extend my sincere and grateful thanks to Prof. Abhineet Anand Head of the Department of Computer Science Department, Galgotias University, Greater Noida, Uttar Pradesh, India.

Attachment

References:-

1) Pleasejing's Weblog .(2007, December 30). Diagram 0 DFD [Online]

Available: http://pleasejing.wordpress.com/2007/12/09/week-4/diagram-0-dfd/ [2011, October 15]

2)https://www.freeprojectz.com/project-synopsis/synopsis-online-banking-system/objective-online-banking-system

2)Sources from the internet.

Authors Profile:-

RAHUL KUMAR, pursuing B.TECH in computer science & engineering and specialization in cloud computing and virtualization in association with "IBM" (2nd year) in "GALGOTIAS UNIVERSITY" .

DOI: 10.18535/ijecs/v6i4.43

DR. ABHINEET ANAND, Assistant Professor at “GALGOTIAS UNIVERSITY” and Program chair of “IBM” courses. (Aug 2016 present),Assistant Professor at ”UPES” (2012 to 2016),Director at “Rashcom Computer Education Pvt. Ltd.”. (Aug 1999 to 2012). *Director at Arpan Assets and Finance Management Pvt. Ltd. Dates Employed Dec 2008 – Jul 2010*. With his 15 years of academic and administrative experience, his research includes following field of endeavor: Decision Tree, nearest neighbor method, Clustering, Rule induction, Optical Fibre Switching in Wavelength Multiplexing, Automata Theory.He has published more than 20 papers in Intentional conference, 4 Intentional Journal, 3 National Journal and 3 National Conference. He has been part 6 special session at various conferences at international level as session chair/co-chair, contributed at 6 different conferences as Technical Program Committee member. His expertise also includes reviewer at more than 10 conferences and Publication group .