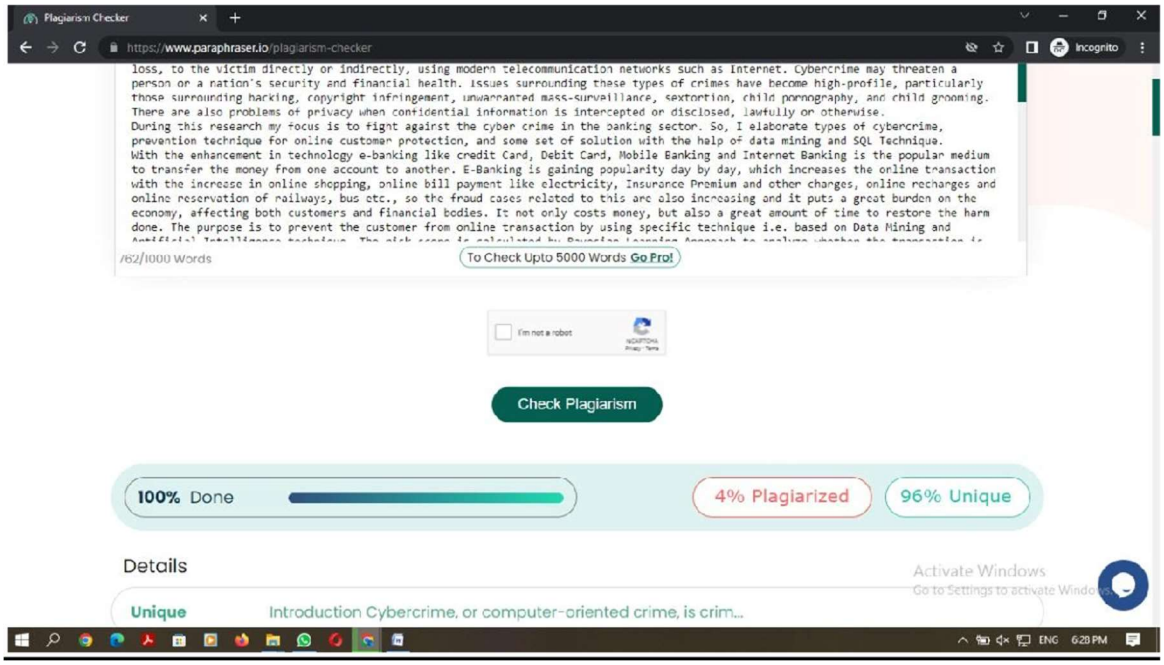
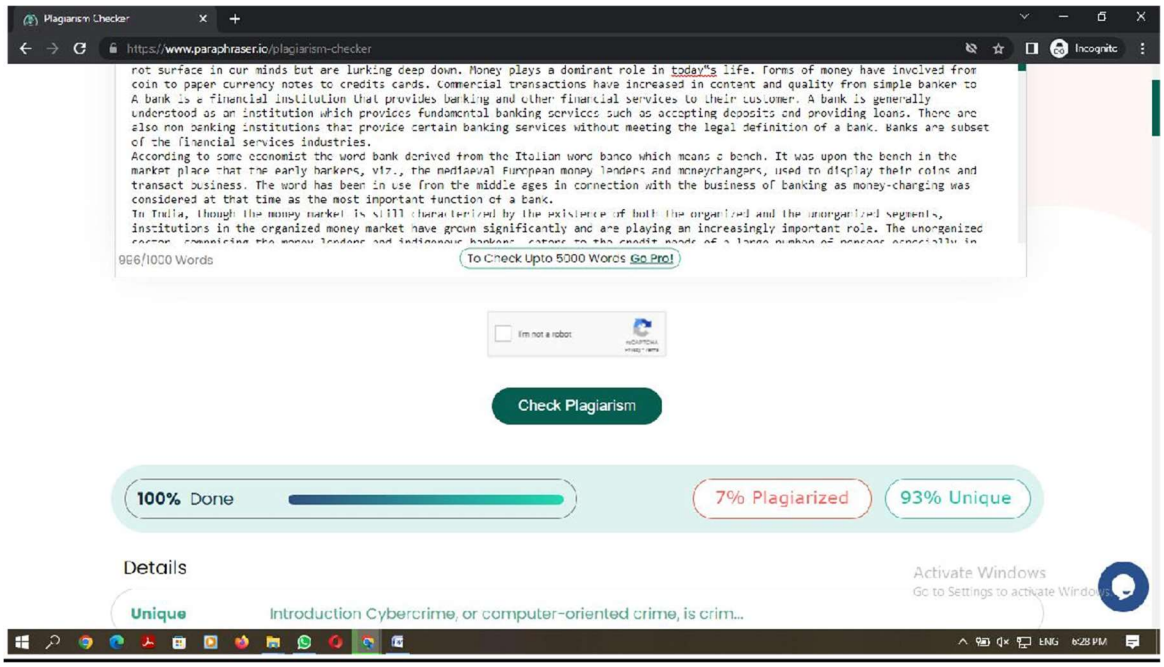
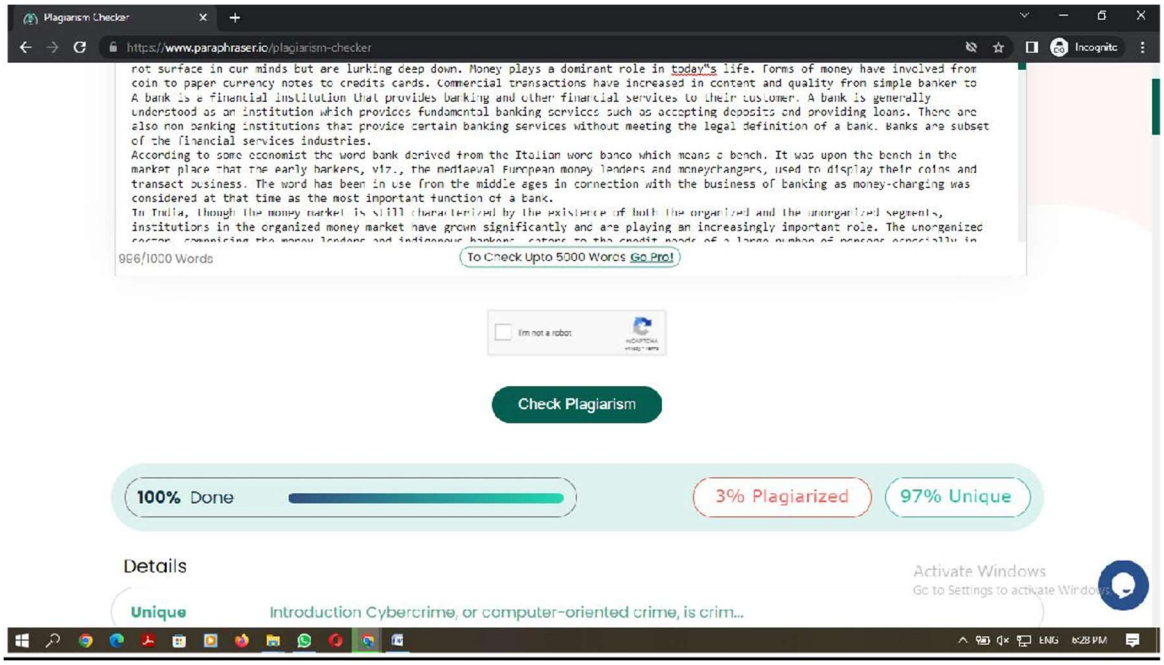
INDEX

Plagiarism Report






Plagiarism Checker
https://www.paraphraser.io/plagiarism-checker
Incognito
rot surface in our minds but are lurking deep down. Money plays a domirant role in today"s life. forms of money have involved from coin to paper currency notes to credits cards. Commercial transactions have increased in content and quality from simple banker to
A bank is a financial institution that provides banking and other financial services to their customer. A bank is generally understood as an institution which provides fundamental banking services such as accepting deposits and providing loans. There are also non banking institutions that provice certain banking services without meeting the legal definition of a bank. Banks are subset of the financial services industries.
According to some economist the word bank derived from the Itolian word banco which means a bench. It was upon the bench in the market place that the early barkers, viz., the mediaeval European money lenders and moneychangers, used to display their coins and transect business. The word has been in use from the middle ages in connection with the business of banking as money-changing was considered at that time as the most important function of a bank.
In India, though the money market is still characterized by the existence of both the organized and the unorganized segments, institutions in the organized money market have grown significantly and are playing an increasingly important role. The unorganized
966/1000 Words
To Check Upto 5000 Words Go Pro!
I'm not a robot
Check Plagiarism
100% Done
3% Plagiarized
97% Unique
Details
Unique
Introduction Cybercrime, or computer-oriented crime, is crim...
Activate Windows
Go to Settings to activate Windows.
ENG
6:28 PM

CHAPTER - I

Introduction

Cybercrime, or computer-oriented crime, is crime that involves a computer and a network.The computer may have been used in the commission of a crime, or it may be the target. Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet. Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, sextortion, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

During this research my focus is to fight against the cyber crime in the banking sector. So, I elaborate types of cybercrime, prevention technique for online customer protection, and some set of solution with the help of data mining and SQL Technique.

With the enhancement in technology e-banking like credit Card, Debit Card, Mobile Banking and Internet Banking is the popular medium to transfer the money from one account to another. E-Banking is gaining popularity day by day, which increases the online transaction with the increase in online shopping, online bill payment like electricity, Insurance Premium and other charges, online recharges and online reservation of railways, bus etc., so the fraud cases related to this are also increasing and it puts a great burden on the economy, affecting both customers and financial bodies. It not only costs money, but also a great amount of time to restore the harm done. The purpose is to prevent the customer from online transaction by using specific technique i.e. based on Data Mining and Artificial Intelligence technique. The risk score is calculated by Bayesian Learning Approach to analyze whether the transaction is genuine or fraudulent based on the two parameters: Customer Spending

Behaviour and Geographical Locations. The customer than spending behaviour that can be identified by KMEAN clustering algorithm and in geographical location the current geographical location is compared with the previous location. If risk score is greater 0.5 then transaction is considered to be fraudulent transactions and then the security mechanism authenticates the user by entering the 4 digit random number that appears on the screen and the genuine user enters the code in a correct manner.

When any crime is committed on the Internet it is termed as cyber crime. Cybercrime generally are of two types:

1. Crimes that target computers directly.
2. Crimes facilitated by computer networks or devices.

When the profit on investment is high and less probability of risk, the people usually want to take advantage of such solution. This is exactly that happen in cyber crime. Obtaining sensitive information and data and using it to perform transactions and to catch such criminals is difficult. Therefore, this has resulted to increase in cyber crime across the world.

Fraud can be defined as the criminal activity i.e. committed by the criminal in order to obtain financial/personal gain. Fraud refers to the act of deceiving the people to obtain the advantage/benefit by using the name of another person.

Banking System Perspective

Banking is today an integral part of our everyday life, At home; at school at office, at business, on travel everywhere we counter some aspect of banking. The significance of banking in our day to day life is being felt increasingly. What are the institutions so inevitable in the present day set up? How do they transact? How did the concept emerge? These are some of the simple queries that do not surface in our minds but are lurking deep down. Money plays a dominant role in today‟s life. Forms of money have involved from coin to paper currency notes to credits cards. Commercial transactions have increased in content and quality from simple banker to speculative international trading, hence the need arose the third party who will assist smooth banding of transaction, mediate between the seller and the buyer hold custody of money and goods, remit funds and also to collect proceeds. He was the "banker" as the number of such mediators grew there is need to control. Such mediating agencies gave birth to the concept of "banks" and "banking".

Banking Industries is the backbone for any economy & is the key indicator to see and analyze the level of development of a country. The Banking sector of India has an annual growth rate of 23 percent, contributing nearly 6 percent of GDP & employing nearly 7.4 million people & has outperformed and most banking indices in the world with highest total returns to shareholders at 36.767. The Indian banks ability to protect assets health through prudent lending helped them emerge from this crisis un scathed. With the exception of the extremely wealthy, very few people buy their homes in all cash transactions. Most of us need a credit in forms of loans, to make such a large purchase. In fact, many people need financial support from bank to fulfill the financial requirement. The world as we know it wouldn‟t run smoothly without credit and banks to issue it.

History of Banking System

The concept of banking was first introduced in medieval Florence in 1397. A powerful family named Medici established a network of shops that allowed patrons to place money on account and withdraw the money in another city that had a Medici

representative. Many powerful families and even the church kept their money in Medici banks. This allowed rich people to travel without the need to carry large number of risk of robbery while travelling. Banking continued to gained popularity throughout Europe by 1700. Nearly every country in Europe had some form of established banking. Modern banking has come a very long way from those humble beginnings in Florence. Banking today covers the entire spectrum of finance from simple savings to credit cards and home loans. Typically, a bank generates profit from transactions fees on financial services or the interest spread on resources it hold in trust for clients while paying them interest on the asset. Banks today are connected electronically so that banking transactions can be made globally in a split second.

A bank is a financial institution that provides banking and other financial services to their customer. A bank is generally understood as an institution which provides fundamental banking services such as accepting deposits and providing loans. There are also non banking institutions that provide certain banking services without meeting the legal definition of a bank. Banks are subset of the financial services industries.

According to some economist the word bank derived from the Italian word banco which means a bench. It was upon the bench in the market place that the early bankers, viz., the mediaeval European money lenders and moneychangers, used to display their coins and transact business. The word has been in use from the middle ages in connection with the business of banking as money-changing was considered at that time as the most important function of a bank.

In India, though the money market is still characterized by the existence of both the organized and the unorganized segments, institutions in the organized money market have grown significantly and are playing an increasingly important role. The unorganized sector, comprising the money-lenders and indigenous bankers, caters to the credit needs of a large number of persons especially in the countryside. Amongst the institutions in the organized sector of the money market, commercial banks and cooperative banks have been in existence for the past several decades.

Before the establishment of banks, the financial activities were handled by money lenders and individuals. At that time the interest rate were very high. Again there were no security of public savings and no uniformity regarding loans. So as to overcome such problems the organized banking sector was established, which was fully regulated by the govt. The organized banking sector works with in the financial system to provide loans, accept deposits and provide other services to their customers. The following are the functions of the bank explain the need of the bank and its importance:-

- To provide the security to the saving of customer.
- To control the supply of money and credit.
- To encourage public confidence in the working of the financial system, increase savings speedily and efficiently.
- To avoid focus of financial powers in the hands of a few individuals and institutions.
- To set equal norms and conditions (i.e. rate of interest, period of lending etc) to all types of customers.

In simple words, bank refers to an institution that deals in money; this institution accepts deposits from the people and gives loans to those who are in need. Besides dealing in money, bank these days perform various functions, such as credit creation agency job and general service. Bank, therefore is such an institution which accepts deposits from the people, gives loans, creates credit and undertakes agency work.

MEANING AND DEFINATION OF BANKING

As we know that people earn money to meet their day to day expenses on food, clothing, education of children and etc. They also need money to meet future expenses on marriage, higher education of children housing building and social functions. These are heavy expenses, which can be met if money is saved out of the

present income. With this practice, savings were available for use where ever needed, but it also involved the risk of loss by theft, robbery and other accidents. Thus, people were in need of a place where money could be saved safely and would be available when required. Banks are such places where people can deposits their savings with the assurance that they will be able to withdraw money from the deposits whenever required. Bank is a lawful organization which accepts deposits that can be withdrawn on demand. It also tends money to individuals and business houses that need it.

- Indian Banking companies Act "Banking companies is one which transacts the business of banking which means the accepting for the purpose of lending or investment of deposits money from the public repayable on demand or otherwise and withdraw able by cheque, draft and order or otherwise".

- Dictionary meaning of word bank The oxford dictionary defines a bank as "an establishment for custody of money received from or on behalf of its customers. Its essential duty is to pay their drafts on it. It"s profits arises from the use of money left employed by them."

- The Webster"s Dictionary defines a bank as "an institution which trades in money, establishment for the deposits, custody and issues of money, as also for making loans and discounts and facilitating the transmission of remittances from one place to another"

- According to Prof. Kinley A bank is an establishment which makes to individuals such advances of money as may be required and safely made, and to which individuals entrust money when it required by them for use"

The above definitions of bank reveal that bank is an business institutions which deals in money and use of money. Thus a proper and scientific definition of the bank should include various functions performed by a bank in a proper manner. We can say that any person, institutions, company or enterprise can be a bank. The business of a bank consists of acceptance of deposits, with drawls of deposits, making loans and advances, investments on a/c of which credit is exacted by banks.

TYPES OF BANKING

Banking is described as the business carried on by an individual at a bank. Today, several forms of banking exist, giving consumers a choice in the way they manage their money most people do a combination of at least two banking types. However, the type of banking a consumer uses normally based on convenience. These are different types of banking through which consumer can attach to it-

(a) Walk-in-Banking

It is still a popular type of banking. As, in the past, it still involves bank tellers and specialized bank officers. Consumers must walk into a bank to use this service normally, in order to withdraw money or deposit it, a person must fill out a slip of paper with the account and specific monetary amount and show a form of identification to a bank letter. The advantage of walk in Banking is the face to face connection between the banker and a letter. Also unlike drive thru and ATM banking, a person can apply for a loan and invest money during a walk in.

(b) Drive thru Banking

It is probably the least popular form of banking today, but is still used enough by consumers to create a need for it. It allows consumers to stay in their while and drive up to a machine equipped with container, chute and intercom. This machine is connected to a bank and is run by one or two bank letters. A person can withdraw or deposit money at a drive thru. He must fill out a slip with his account and specific monetary amount and put it in the container. The container travels through the chute to the bank letter, who will complete the banker‟s request. This is where the intercom comes into play. The bank teller and banker use it to communicate and discuss the specific banking request.

(c) ATM Banking

It is very popular because it gives a person 24 hour access to his bank account. Walk in and drive thru banking does not offer this perk. In order to use an ATM, a person must have an ATM card with personal identification number (PIN) and access to an

ATM machine. Any ATM machine can be used, but charges apply if the ATM machine is not affiliated with the bank listed on the ATM card. By sliding an ATM card into an ATM machine, it is activated and then through touching buttons on the machine, a consumer is able to withdraw or deposit money.

(d) Online Banking

It allows a person to get on the internet and sign into their bank. This process is achieved with the use of a PIN, different from the one used for the ATM card. By going website of a bank and entering it, a consumer can get into his account, withdraw money, deposit money, pay bills, request loans and invest money. Online banking is growing in popularity because of its convenience. These different types of banking give a consumer the power of choice and also give them a comfortable banking system that gives them a convenient choice.

Competition and the constant changes in technology and lifestyles have changed the face of banking. Now days, banks are seeking alternative ways to provide and differentiate amongst their varied services. Customers, both corporate as well as retail, are no longer willing to queue in banks, or wait on the phone, for the basic banking services. They demand and except a facility to undertake their banking activities where and when they wish to do.

Internet Banking refers to a system allowing individual customers to perform banking activities at off bank sites such as home, office and their other locations via internet based secured networks. Internet or on line banking through traditional banks enable customers to perform all routine transactions, such as account transfer, balance inquiries, bill payments and stop-payment requests, and some even offer online loan and credit card applications.

Strides in the field of technology have redefined the role and structure of an IT department in a Bank. Rapid strides in the field of technology redefined the use of technology in banking. The fact that using better technology and systems, banks can garner more customers, retain existing ones and channel more of the customers business to its counters has forced business department to now look at IT as an

effective marketing tool. On the operational side, the power of IT in reducing transaction costs, providing better customer service and offering an over-all customer convenience has basically made this a win-win situation for both banks as well as its clients. These have become the main drivers for getting IT the importance it has got in banks in recent times. The nerve centre of technology in a bank‟s IT dept. is the „Core Banking System‟.

CORE BANKING SYSTEM

Core banking systems are basically the heart of all systems running in a bank and it forms the Core of the bank's IT platform. Amongst other functionalities, it provides the customer information management, central accounting and the transaction-processing functions, which by far are the most fundamental processes in a bank. With the advancement in technology and with passage of time, core systems now-days tend to cover more and more functionality giving the bank an integrated solution for most of its operations in different business lines. Alongside, it also provides a central operational database of customers' assets and liabilities giving facility to generate a 360 degree view of the customer‟s relationship with the bank, which is fundamental for the CRM strategy of the bank. Core banking systems reside either in the heart of a bank's data center or in other words can also be termed as the heart of the data-centre itself.

Element of core banking system

By and large a typical traditional core banking system would be composed of four components:

- Customer Information File
- General Ledger System
- Transaction processing
- Basic Management information system (MIS) reporting.

Advantage of core banking system

Following are the advantages of core banking system are:

- Limited Professional Manpower to be utilized more effectively.
- Customer can have anywhere, more convenient and easier banking.
- ATM, Internet Banking, Mobile Banking, Payment Gateways, Referral Business.
- More Strong and economical way for MIS.
- Reduction in Branch Manpower by 15-20%.
- Additional Manpower available for Marketing, Recovery and Personalized banking.
- Instant Information availability for decision support.
- Quick and Accurate Implementation of Policies.
- Improved Recovery Process causing reduction on recovery costs, NPA Provisions.
- Innovative, redefined or improved processes (e.g. Inter Branch Reconciliation) causing reduction in Manpower at Head Office Reduction in Software maintenance at Branch and Head Office.
- Centralized Printing and Back up resulting in reduction in capital and revenue expenditure on printing and backup devices and media at branches.
- Electronic Transactions with Other Financial Institutions.
- Increased Speed in working resulting in more business opportunities and reduction in penalties, legal expenses etc.

Disadvantage of core banking system

Following are the disadvantage of core banking system are:

- The technology must be upgraded every time and if some more errors occur in some part whole system may be disrupted.

- If data is not protected properly and if proper care is not taken, hackers can gain access to the sensitive data.

- Hackers are easily mischief and hacked the accounts of customer for which a lot of fraud has been made easy in cyber banking system.

- Most data entry operation are out sourced and validity of such massive data is questionable.

In the present globalizes scenario, information technology is the most important and controversial term. It is the most powerful technology which is fast, quick and accurate in all sectors. Increased use of information and communication technology (ICT) such as computers, mobile phones, Internet, and other associated technologies are the routes which gave emergence to lot of constructive work as well as destructive work. The destructive activities are considered as electronic crime which includes spamming, credit card fraud, ATM frauds, Money laundering, Phishing, Identity theft, denial of service and other host contributing crime in the Indian Banking sector. Computers and Internet are also the new powerful information tools in present era, these new technologies brings out new threats opportunities such as denial of service attacks, viruses, unauthorized entry, information tampering, cyber stalking, spamming, paper-jacking, dumping or phone-napping and computer damage . These disadvantages lead to frauds and crimes in banks.

FRAUDS AND CRIMES IN BANKING SECTORS

Definition of Fraud

Fraud is the dishonest act and behavior by which one person gains or intends to gain an advantage over another person. The gain may accrue to the person himself or to someone else. Fraud causes loss to the victim, directly or indirectly. In earthly terms bank frauds include all sort of misappropriations, embezzlements, and manipulations

of negotiable instruments. Frauds also include misrepresentations, cheating, thefts, undue favors and irregularities.

Fraud is defined as any behaviour by which one person intends to gain a dishonest advantage over another. In other words, fraud is an act or omission which is intended to cause wrongful gain to one person and wrongful loss to the other, either by way of concealment of facts or otherwise.

Section 421 Indian penal code defines Fraud as whoever dishonestly or fraudulently removes, conceals or delivers to any person, or transfer or causes to be transferred to any person, without adequate consideration, any property, intending thereby to prevent, or knowing it to be likely that he will thereby prevent, the distribution of that property according to law among his creditors or the creditors of any other person, shall be punished with imprisonment of either description for a term which may extend to two years or with fine or with both"

"Definition of word "FRAUD"U/S 17 of Indian contract Act"

"Fraud" means and includes any of the following acts committed by a party to a contract, or with his connivance or by his agent, with intent to deceive another party thereto his agent, or to induce him to enter into the contract:

i) the suggestion, as a fact of that which is not true or by one who does not believe it to be true.

ii) the active concealment of a fact by one having knowledge or belief of the fact:

iii) a promise made without any intention of performing it:

iv) any other act fitted to deceive; and

v) any such act or omission as the law specially declares to be fraudulent.

However, mere silence as to the facts likely to affect the willingness of a person into a contract is not fraud unless there is a duty to speak or his silence is, itself, equivalent to speech.

Fraud is defined U/S 421 of the Indian penal code and u/s 17 of the Indian contract act. Thus essential elements of frauds are:

i) There must be a representation and assertion;

ii) It must relate to a fact;

iii) It must be with the knowledge that it is false or without belief in its truth; and

iv) It must induce another to act upon the assertion in question or to do or not to do certain act.

Bank Fraud

Bank fraud is the use of fraudulent means to obtain money, assets, or other property owned or held by a financial institution, or to obtain money from depositors by fraudulently representing to be a bank or financial institution. In many instances, bank fraud is a criminal offense. While the specific elements of a particular banking fraud law vary between jurisdictions, the term bank fraud applies to actions that employ a scheme or artifice, as opposed to bank robbery or theft. For this reason, bank fraud is sometimes considered a white-collar crime

The number of bank frauds in India is substantial. It in increasing with the passage of time. All the major operational areas in banking represent a good opportunity for fraudsters with growing incidence being reported under deposit, loan and inter-branch accounting transactions, including remittances.

Bank fraud is a big business in today‟s world. With more educational qualifications, banking becoming impersonal and increase in banking sector have gave rise to this white collar crime. Different Frauds against banks are classified as below:

Stolen cheques

Some fraudsters obtain access to facilities handling large numbers of cheques, such as a mailroom or post office or the offices of a tax authority (receiving many checks) or a corporate payroll or a social or veterans' benefit office (issuing many cheques). A few cheques go missing; accounts are then opened under assumed names and the cheques (often tampered or altered in some way) deposited so that the money can then be withdrawn by thieves. Stolen blank cheque books are also of value to forgers who then sign as if they were the depositor

Cheque kiting

Cheque kiting exploits a system in which, when a cheque is deposited to a bank account, the money is made available immediately even though it is not removed from the account on which the cheque is drawn until the cheque actually clears.

Forgery and altered cheques

Thieves have altered cheques to change the name (in order to deposit cheques intended for payment to someone else) or the amount on the face of a cheque (a few strokes of a pen can change Rupees 100.00 into Rupees 100,000.00, although such a large figure may raise some eyebrows).

Instead of tampering with a real cheque, some fraudsters will attempt to forge a depositor's signature on a blank cheque or even print their own cheques drawn on accounts owned by others, non-existent accounts or even alleged accounts owned by non-existent depositors. The cheque will then be deposited to another bank and the money withdrawn before the cheque can be returned as invalid or for non-sufficient funds.

Accounting fraud

In order to hide serious financial problems, some businesses have been known to use fraudulent book keeping overstating sales and income, inflating the worth of the company‟s assets or stating a profit when the company is operating at a loss. These tampered records are then used to seek investment in the company's bond or security issues or to make fraudulent loan applications in a final attempt to obtain more money

to delay the inevitable collapse of an unprofitable or mismanaged firm. Examples of accounting frauds: Enron and WorldCom. These two companies "cooked the books" in order to appear as they had profits each quarter when in fact they were deeply in debt.

Uninsured deposits

There are a number of cases each year where the bank itself turns out to be uninsured or not licensed to operate at all. The objective is usually to solicit for deposits to this uninsured "bank", although some may also sell stock representing ownership of the "bank". Sometimes the names appear very official or very similar to those of legitimate banks. For instance, the "Chase Trust

Bank" of Washington D.C. appeared in 2002 with no license and no affiliation to its seemingly apparent namesake; the real Chase Manhattan Bank is based in New York. Accounting fraud has also been used to conceal other theft taking place within a company.

Demand draft fraud

Demand draft fraud is usually done by one or more dishonest bank employees. They remove few DD leaves or DD books from stock and write them like a regular DD. Since they are insiders, they know the coding, punching of a demand draft. These Demand drafts will be issued payable at distant town/city without debiting an account. Then it will be cashed at the payable branch. For the paying branch it is just another DD. This kind of fraud will be discovered only when the head office does the branch-wise reconciliation, which normally will take 6 months. By that time the money is unrecoverable.

Rogue traders

A rogue trader is a highly placed insider nominally authorised to invest sizeable funds on behalf of the bank; this trader secretly makes progressively more aggressive and risky investments using the bank's money, when one investment goes bad, the rogue

trader engages in further market speculation in the hope of a quick profit which would hide or cover the loss.

Unfortunately, when one investment loss is piled onto another, the costs to the bank can reach into the hundreds of millions of dollars; there have even been cases in which a bank goes out of business due to market investment losses.

Some of the largest bank frauds ever detected were perpetrated by currency traders John Rusnak, and Nick Leeson. Jerome Kerviel, allegedly defrauded Societe Generale of 4.9 billion euros ($7.1 billion) us dollars, while trading stock derivatives.

Fraudulent loans

One way to remove money from a bank is to take out a loan, a practice bankers would be more than willing to encourage if they know that the money will be repaid in full with interest. A fraudulent loan, however, is one in which the borrower is a business entity controlled by a dishonest bank officer or an accomplice; the "borrower" then declares bankruptcy or vanishes and the money is gone. The borrower may even be a non-existent entity and the loan merely an artifice to conceal a theft of a large sum of money from the bank.

Fraudulent loan applications

These take a number of forms varying from individuals using false information to hide a credit history filled with financial problems and unpaid loans to corporations using accounting fraud to overstate profits in order to make a risky loan appear to be a sound investment for the bank.

Forged or fraudulent documents

Forged documents are often used to conceal other thefts; banks tend to count their money meticulously so every penny must be accounted for. A document claiming that a sum of money has been borrowed as a loan, withdrawn by an individual depositor or transferred or invested can therefore be valuable to a thief who wishes to conceal the minor detail that the bank's money has in fact been stolen and is now gone.

Wire transfer fraud

Wire transfer networks such as the international SWIFT interbank fund transfer system are tempting as targets as a transfer, once made, is difficult or impossible to reverse. As these networks are used by banks to settle accounts with each other, rapid or overnight wire transfer of large amounts of money are commonplace; while banks have put checks and balances in place, there is the risk that insiders may attempt to use fraudulent or forged documents which claim to request a bank depositor's money be wired to another bank, often an offshore account in some distant foreign country.

There is a very high risk of fraud when dealing with unknown or uninsured institutions.

The risk is greatest when dealing with offshore or Internet banks (as this allows selection of countries with lax banking regulations), but not by any means limited to these institutions. There is an annual list of unlicensed banks on the US Treasury Department site which currently is fifteen pages in length.

Bill discounting fraud

Essentially a confidence trick, a fraudster uses a company at their disposal to gain confidence with a bank, by appearing as a genuine, profitable customer. To give the illusion of being a desired customer, the company regularly and repeatedly uses the bank to get payment from one or more of its customers. These payments are always made, as the customers in question are part of the fraud, actively paying any and all bills raised by the bank. After time, after the bank is happy with the company, the company requests that the bank settles its balance with the company before billing the customer. Again, business continues as normal for the fraudulent company, its fraudulent customers, and the unwitting bank. Only when the outstanding balance between the bank and the company is sufficiently large, the company takes the payment from the bank, and the company and its customers disappear, leaving no-one to pay the bills issued by the bank.

Payment card fraud

Credit card fraud is widespread as a means of stealing from banks, merchants and clients.

Booster cheques

A booster cheque is a fraudulent or bad cheque used to make a payment to a credit card account in order to "bust out" or raise the amount of available credit on otherwise-legitimate credit cards. The amount of the cheque is credited to the card account by the bank as soon as the payment is made, even though the cheque has not yet cleared. Before the bad cheque is discovered, the perpetrator goes on a spending spree or obtains cash advances until the newly-"raised" available limit on the card is reached. The original cheque then bounces, but by then it is already too late.

Stolen payment cards

Often, the first indication that a victim's wallet has been stolen is a phone call from a credit card issuer asking if the person has gone on a spending spree; the simplest form of this theft involves stealing the card itself and charging a number of high-ticket items to it in the first few minutes or hours before it is reported as stolen.

A variant of this is to copy just the credit card numbers (instead of drawing attention by stealing the card itself) in order to use the numbers in online frauds.

Duplication or skimming of card information

This takes a number of forms, ranging from a dishonest merchant copying clients' credit card numbers for later misuse (or a thief using carbon copies from old mechanical card imprint machines to steal the info) to the use of tampered credit or debit card readers to copy the magnetic stripe from a payment card while a hidden camera captures the numbers on the face of the card.

Some thieves have surreptitiously added equipment to publicly accessible automatic teller machines; a fraudulent card stripe reader would capture the contents of the magnetic stripe while a hidden camera would sneak a peek at the user's PIN. The

fraudulent equipment would then be removed and the data used to produce duplicate cards that could then be used to make ATM withdrawals from the victims' accounts.

Empty ATM envelope deposits

A criminal overdraft can result due to the account holder making a worthless or misrepresented deposit at an automated teller machine in order to obtain more cash than present in the account or to prevent a check from being returned due to non-sufficient funds. United States banking law makes the first $100 immediately available and it may be possible for much more uncollected funds to be lost by the bank the following business day before this type of fraud is discovered. The crime could also be perpetrated against another person's account in an "account takeover" or with a counterfeit ATM card, or an account opened in another person's name as part of an identity theft scam. Later this decade, this scenario may become a thing of the past due to the emergence of ATM deposit technology that scans currency and checks without using an envelope.

Impersonation

Impersonation has become an increasing problem; the scam operates by obtaining information about an individual, then using the information to apply for identity cards, accounts and credit in that person's name. Often little more than name, parents' name, date and place of birth are sufficient to obtain a birth certificate; each document obtained then is used as identification in order to obtain more identity documents. Government-issued standard identification numbers such as "social security numbers" are also valuable to the fraudster.

Information may be obtained from insiders (such as dishonest bank or government employees), by fraudulent offers for employment or investments (in which the victim is asked for a long list of personal information) or by sending forged bank or taxation

correspondence. Some fictitious tax forms which purported to have been sent by banks to clients in 2002 were:

- W-9095 Application Form for Certificate Status/Ownership for Withholding Tax
- W-8BEN Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding
- W-8888 The actual origin of these forms is neither the bank nor the taxman - they're sent by would-be identity thieves and W-8888 doesn't exist, W-9095 is also fictitious (the real W-9 asks much less info) and W-8BEN is real but may have been tampered to add intrusive additional questions. The original forms on which these fakes were based are intended to collect information for income tax on income from deposits and investment.

In some cases, a name/SIN pair is needed to impersonate a citizen while working as an illegal immigrant but often the identity thieves are using the bogus identity documents in the commission of other crimes or even to hide from prosecution for past crimes. The use of a stolen identity for other frauds such as gaining access to bank accounts, credit cards, loans and fraudulent social benefit or tax refund claims is not uncommon.

Unsurprisingly, the perpetrators of such fraud have been known to take out loans and disappear with the cash, quite content to see the wrong persons blamed when the debts go bad or the police come calling.

Some corporations have engaged in over-expansion, using borrowed money to finance costly mergers and acquisitions and overstating assets, sales or income to appear solvent even after becoming seriously financially overextended.

Prime bank fraud

The "prime bank" operation which claims to offer an urgent, exclusive opportunity to cash in on the best-kept secret in the banking industry, guaranteed deposits in "prime banks", "constitutional banks", "bank notes and bank-issued debentures from top 500

world banks", "bank guarantees and standby letters of credit" which generate spectacular returns at no risk and are "endorsed by the World Bank" or various national governments and central bankers. However, these official-sounding phrases and more are the hallmark of the so-called "prime bank" fraud; they may sound great on paper, but the guaranteed offshore investment with the vague claims of an easy 100% monthly return are all fictitious financial instruments intended to defraud individuals.

ELECTRONIC CRIME

Electronic crime started during the period of 1960 in the form of Hacking. In the period of 1970 presence of computer introduced new crimes as computer crimes in the form of privacy violation, phone tapping, trespassing and distribution of illicit materials. Then, later in the period of 1980‟s electronic systems crime emerges in the form of software piracy, copyright violations and introduction of viruses. The extent of damage after 1980‟s increased due to the highly sophisticated electronic systems. These electronic crimes gave a wider impact on the Indian market, international market, Banking sector and other areas also. Therefore, presently electronic crime became a major subject of concern worldwide.

The concept of Electronic Crime is a vital aspect. Since new information is available in an unbiased manner it is often not possible to detect crime on the basis of that information. In the paper, researchers make an attempt to study the Electronic crimes and major crimes of Indian banking sector. In the present globalize scenario, Information Technology is the factor responsible of further growth and development in the Indian banking sector. In this speedy world, customers often feel insecure and reluctant about there banking transactions especially in e-banking or online banking. Technology has emerged as the lifeblood in today Indian Banking sector whether private and public sector banks. Presently, banking sector primarily focus on customer satisfaction the fulfillment of their need and satisfaction in most effective manner. With the introduction of „Electronics‟ in the banking system several problems are emerged as

- Hacking and Stealing of data
- Failure of ATMs
- Money laundering
- Credit card theft 8

Electronic Crime – An Overview

Computers, Internet and other electronic medium are the commanding information tools to make possible immediate exchange and distribution of data, images and materials. Information Technology brings growth and development and its fraudulent practices are bitterly termed as cyber-crime or computer crime, e-crime, hi-tech crime or Electronic crime. These all activities are directly associated with illegal activities in which a computer or Internet network is working as a medium, source, tool, target or place of a crime.

Computer and Internet are the powerful in a row tools including financial networks, communication systems, power stations, modern automobiles and appliances. These computers networks records withdrawals, deposits, purchases, telephone calls, usage of electricity, medical treatments, driving patterns and lot more. Quite a few innovative technologies are also extensively available which are responsible for causing electronic crime. They are denial of service attacks, viruses, unauthorized entry, information tampering, cyber stalking, spamming, paper-jacking, dumping or phone-napping and computer damage. The internet services and web technologies in India is growing at a fast level. This increased growth gave rise to new opportunities. These technologies have its own pros and cons. The pros are the benefits and advantages but the cons are named as Cyber crime or Electronic Crime. These crimes take place due to certain loop-holes – which result in e-mail espionage, credit card fraud, spams, software piracy etc.

Electronic Crime in Banking Sector

Banking system is the lifeblood and backbone of the economy. Information Technology has become the backbone of the banking system. It provides a tremendous support to the ever – increasing challenges and banking requirements. Presently, banks cannot think of introducing financial product 161 Int. Electronic crimes are illegal activities committed by means of computer end of the criminal activity can be either a computer, network operations. Electronic crimes are genus of crimes, through computers and its networks. Electronic crime is a crime that is committed online in several areas with e-commerce. A computer can be the target of an offence when unauthorized access of computer network occurs and on other hand it affects E-COMMERCE. Electronic crimes can be of a variety of types such as Telecommunications Piracy, Electronic Money Laundering and Tax Evasion, Sales and Investment Fraud, Electronic Funds Transfer Fraud etc. The Indian Banking sector is riding up with numerous revolutionary changes to transform the "Brick-and-mortar" bank branches to a modified network system in "core banking solutions". The banking sector consists of public sector, private sector and foreign banks. With this a number of IT based banking products services and solutions are available –

- Phone Banking
- ATM facility
- Credit, Debit and Smart cards
- Internet banking
- Mobile Banking
- SWIFT Network
- INFINET Network etc

The present contemporary epoch has replaced these traditional monetary instruments from a paper and metal based currency to "plastic money" in the form of credit cards, debit cards, etc. This has resulted in the mounting use of ATM all over the world. The

utilize of ATM is not only safe but also convenient but safety and convenience, unfortunately, has an evil side. This evil side is reflected in the form of "ATM frauds".

Credit card fraud has become ordinary on internet which not only affects card holders but also online merchants. Credit card fraud can be completed by taking over the account, skimming or if the card is stolen. The term "Internet fraud" refers usually to any type of fraud scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, or Websites - to existing fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to broadcast the proceeds of fraud to financial institutions or to other connected with the scheme.9

Further studies on the electronic crime shows that- it can be categorized in two major ways Computer device used as a medium of target to commit crime- Electronic crime is used as a target to commit crime in includes

- Sabotage of computer systems or computer networks
- Sabotage of operating systems and programmes
- Theft of data/ information
- Theft of intellectual property such as computer software
- Theft of marketing information
- Blackmail based on information gained from computerized files, such as medical information, personal history, financial data etc

Computer is working as an instrument of the crime – Banking criminals are using various electronic medium such as internet, e-mail, and flash encrypted messages etc to commit crime. This crime through computer network takes place in the banking sector. They are

- Fraudulent use of Automated Teller Machine (ATMs) cards and accounts
- Credit card frauds

- Frauds involving electronic funds transfers (EFTs)
- Telecommunication frauds
- Frauds relating to E-commerce and EDI

Reasons for Electronic Crime

Computers are exposed, therefore, the law is mandatory to protect and safeguard them against cyber crime or electronic crime. The reasons for the exposure of computers may as follows:

Competence to accumulate data: The computer has exclusive characteristic of storing data in a very comparatively small space this makes the user more comfortable to steal the data either physically or virtually through any electronic medium.

Unproblematic to Approach: The trouble encountered in guarding a computer system from unauthorized access is that there is every opportunity of breach due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

Complex: The computers effort on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

Negligence: Negligence is directly associated with human behavior. While protecting the computer system it is possible there might be any negligence, which change direction provides of the cyber criminal to gain access and control over the computer system.

Loss of Proof: Loss of evidence facts & figures is a very common obvious problem as all the data are normally destroyed. This loss of evidences leads to paralyses of the entire computer system.

Electronic Crime in Indian Banking Sector

E banking is 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 personal computer and a mobile phone with browser or desktop software, telephone or digital television

Credit card Fraud- A major kind of electronic crime is credit card fraud. Indian banking sector is introducing new innovations against counterfeiting and fraud, which are highly sophisticated to profiting from or beating these systems. Most of the credit card fraud is committed with the use of counterfeited cards. Credit card fraud is also termed as „Identity Theft‟ in which a person may use the identity of other person for exercising fraud or deception. Credit card fraud in banking sector can be committed as

- Use of unauthorized account or personal information to consider as an act of criminal deception
- Illegal or unauthorized use of account for personal gain
- Misrepresentation of account information to obtain services

Several new security measures are introduced to gradually to reduce the credit card fraud in one part but it swiftly shifts to other part. Therefore, the problem of credit card fraud is serious and occurring by stealing the cards and the accompanying information at the time of transaction delivery.

Money Laundering: Throughout the precedent two decades, IT and Internet technologies have reached each one nook and corner of the world. E-commerce has come into existence due to the attributes of Internet like ease of use, speed, anonymity and its International nature. Internet has transformed the planet into a frontier excluding market place that never sleeps. Computer networks and Internet authorize relocate of funds electronically between trading partners, businesses and consumers.

This shift can be done in many ways like use of credit cards, Internet banking, e-cash, e- wallet etc. for example, smart cards. In some other forms of computer-based e-money, there is no upper limit.

Two persons also can shift funds in a straight line using e- wallets. This problem is further compounded by the fact that, in several countries, non-financial institutions are also allowed to issue e-money. Monitoring the behavior of these institutions in a habitual manner is not possible. Earlier, cross-border transactions were controlled by the central banks of respective countries. With the entrance of Internet commerce, the jurisdictional technicalities come into battle and it is another area that is being exploited by the money launderers. The competence to transfer limitless amounts of money without having to go through strict checks makes cyber money laundering an attractive proposition.

The main objective of these guidelines is to prevent the banking transactions from being used by criminal intentionally or unintentionally as an element of money laundering. Banks and financial institutions are the core targets or focus on anti-money laundering practices and combating of financial terrorism laws due to their vulnerability and adherence of these laws to combat money laundering a counter financing. The money laundering reduces the officially authorized quantity of the banks business causes fluctuations in the exchange rate. Money laundering can undermine the credibility of the banking system. Facilitating the activities of launderers even inadvertently can set in motion the banks into problems with law enforcement agencies and also governments.

ATMs Frauds: Over the past three decades, large number of banking customers depends on the ATM to conveniently meeting their banking needs. In the recent years, there have been a large number of accidents of ATMs frauds. It is necessary to manage the risk associated with ATM fraud as well as diminishing its impact on the important issues that face financial institutions as fraud techniques to become more advanced with increased occurrences.

The prevailing contemporary era has replaced long-established monetary instruments from a paper and metal based currency to “plastic money” in the form of credit cards, debit cards, etc. This has resulted in the escalating utilize of ATM all over the world. The use of ATM is not only safe and sound but also suitable. This safety and convenience, has an evil side which is reflected in the form of “ATM FRAUDS” that is an international problem. The use of plastic money is increasing for payment of shopping bills, electricity bills, school fees, phone bills, insurance premium, traveling bills and even petrol bills. The convenience and safety that credit cards carry with its use has been instrumental in increasing both credit card volumes and usage. This growth is not only in positive use of the same but as well as the negative use of the same. The world at large is struggling to increase the convenience and safety on the one hand and to reduce it misuse on the other. A few of the accepted techniques used to carry out ATM crime in banks are:

- ATM‟s card reader is tampered with in order to trap a customer‟s card through card jamming.

- Card Skimming is the unlawful technique of stealing the card‟s security information from the card‟s magnetic stripe.

- Card Swapping, is another technique in which customer‟s card is swapped with another card without the knowledge of cardholder.

- Website Spoofing, here a fresh fabricated site is prepared which looks valid to the user and customers are asked to give their card number PIN and other information, which are used to reproduce the card for use at an ATM.

- ATM machine is physical attacked for removing the cash

Need and Significance of the problem

Due to the growth of modern technology, the mode of payment of individual has changed significantly. The use of Online Payment mode such as Online Banking, Debit Card, Credit Card etc. has become popular and is becoming important in day to day activities because it allows bank customers to purchase goods and services from the shopping websites or from the market.

Fraud deals with cases that happen due to criminal purpose which are difficult to identify. Fraud can be mainly divided into two types:

- **Offline Fraud:** Most of the offline fraud incidents occur due to the steal of purse/wallet that contains important documents. Documents such as Driving License, ID card etc. contains crucial information such as name, date of birth, transaction slips etc.

- **Online Fraud:** Online fraud occurs when fraudster present their website as a genuine website in order to obtain crucial personal data of a customer and perform illegal transactions on such customer account.

Credit card is also one of the most illegal types of fraud. Credit Card is a plastic card i.e. issued to customers of a bank as one of the mode of payment. It allows cardholders to purchase goods and services from the shopping websites or from the market. Credit Card Fraud is defined as, when an individual uses another individual credit card for personal use while the owner of the card as well as the card issuer are not aware of the thing that the card is being used.

Statement of the problem

1. What is online Customer Protection Policy in the case of Indian Banking System?
2. How to monitor customer behavior and activities during online transaction or surfing?
3. How Data Mining beneficial for manage the fraud on internet?
4. What is the technique used by Indian Banking System to prevent online fraud?
5. What is the meaning of online fraud and how to prevent it effectively for banking sector?

CHAPTER – II

Review of Related Literature

Srivastva.Abhinav, HMM (Hidden Markov Model) is proposed to detect fraudulent transactions which is initially trained with the normal behavior of a cardholder therefore if an incoming credit card transaction is not accepted by the HMM with sufficiently high probability, it is considered to be fraudulent and K Mean Clustering algorithm is used to identify spending behavior of a customer. HMM-based applications are used in various areas such as speech recognition, bioinformatics, and genomics so this model is able to detect fraud in large volumes of transactions.

Panigrahi.Suvasin, Fraud Detection System is proposed i.e. based on the combination of three approaches: Rule-based filtering, Dempster–Shafer theory and Bayesian learning in which Dempster rule is used to match customercurrent behavior compared with the previous behavior ,rule based filtering approach is used to determine the suspicious level of each incoming transaction and Bayesian learning approach is used to update the suspicious score of transaction using history database of both genuine cardholder as well as fraudster.

Sanchez's, Association rules (Fuzzy Rules) are used to detect new, undesired behavior of bank customer in the online verification process and Association Rules (Fuzzy Rules) are applied in the area of Business Management and planning to extract data of fraudulent transaction from a large database.

Farvaresh.Hamid, a framework was proposed to detect fraud telecommunication subscribers by using various techniques such as data cleaning, dimension reduction, clustering and classification and the main problem in this framework is that it requires the historic data to identify whether the customer is fraudster or genuine.

CHAPTER – III

RESEARCH METHODOLOGY

Research Question

1. What is the meaning of online fraud and how to prevent it effectively for banking sector?
2. What is online Customer Protection Policy in the case of Indian Banking System?
3. How to monitor customer behavior and activities during online transaction or surfing?
4. How Data Mining beneficial for manage the fraud on internet?
5. What is the technique used by Indian Banking System to prevent online fraud?

Objective of the study

- To know details about online fraud, types of online fraud and how to prevent it effectively for banking sector.
- To find significant difference in fraud technique generally used in banking sector.
- To find the relationship and benefits related to Data Mining, protection policy, fraud etc.
- To find the solution to prevent online fraud in banking sector using data mining, SQL server database, SQL injection.

Hypothesis of the study

Null Hypothesis used for this research topic: "A Study of Cyber Crime in Banking System to Prevent Online Fraud with the help of Data Security Techniques with Reference of HDFC Bank New Delhi"

Operational Definition of key terms

Methods to Steal Personal Information:

There are various methods or techniques that cyber criminals used to commit the crime:

Hacking: Hacker is a person who seeks and exploits weakness in computer system. Attacker breaks into industry or personal databases.

Phishing: Phishing is a fraudulent attempt, usually madethrough email, to steal your personal information.

Spoofing: The word "spoof" means to hoax, trick, or deceive. Spoofing refers to tricking or deceiving the computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet.

Spyware: The computer user unknowingly downloads software from the Internet that contains spyware. Spyware collects personal information from your computer and transmits it to fraudster or attacker.

Shoulder Surfing: An attacker watches a bank customer from a nearby location as the customer punches in his personal information. If the customer is giving his personal information over the phone (e.g., to a hotel or car rental company), the attacker may listen to the conversation so as to obtain personal information of bank customer

Dumpster Diving: An attacker goes through a customer‟s garbage cans or trash bins to obtain personal information of bank customer such as bank statement, payment receipt etc.

Methodology

For this study stratified sampling was employed. The focus of this research was **Indian Banking System and their associated Customers.**

Primary Sources

The population was divided into strata which consisted of the below branch of HDFC banks.

Selected Branch:

HDFC BANK Ltd
Address: No 8 A, Milap Niketan, Bahadur Shah Zafar Marg, ITO, New Delhi, Delhi 110002
Contact No - 022 6846 1208

50 Customers will select randomly for this research.

Secondary Sources

Apart from Primary sources Researcher will use secondary sources like

- Historical Reports Indian Banking System and respective bank website.
- Data also collected using Internet & Website of HDFC Bank
- Books & Magazine
- News Paper & Print Media
- TV & Digital Media also helpful for research

Why Secondary Data Required?

Secondary data refers to data that was collected by someone other than the user. Common sources of secondary data include censuses, information collected by government departments, organisational records and data that was originally

collected for other research purposes. Primary data, by contrast, are collected by the investigator conducting the research.

Secondary data analysis can save time that would otherwise be spent collecting data and, particularly in the case of quantitative data, can provide larger and higher-quality databases that would be unfeasible for any individual researcher to collect on their own.

Variable of the study

In a research study, independent variables are antecedent conditions that are presumed to affect a dependent variable. They are either manipulated by the researcher or are observed by the researcher so that their values can be related to that of the dependent variable.

So, in this research variables may be

- Customer Psychological factors
- Awareness Ratio related to Bank Fraud
- number of hours devoted on banking website
- Browsing style
- Knowledge of Banking Interface
- Knowledge of Online Fraud

Population of the study

Sample Size:50

Sample Location: New Delhi, India

Characteristics of the sample: Sample will be Customer of HDFC Bank in New Delhi, India.

Tools Used for the Study

The researcher will collect primary data in the field work.

But for representation of data and analysis following software will use:

Ms Excel - for data collection and chart presentation,

Ms. Paint - for drawing and image editing purpose.

Spss- Apart from that SPSS Can be used for analysis purpose

Techniques going to be used

Data Mining:

Data Mining is a technique that uses statistical, artificial intelligence, and neural network technique to extract and fetch useful information from a large database. Data Mining is a technique to study data from different views and summarizes it into crucial information. Data Mining is a technique that is used to detect financial fraud detection because it can identify new attacks before financial fraud can be detected by human experts.

Challenges in Data Mining to detectFraud:

- There are millions of transactions each day. To extract large amount of data from a database requires highly efficient techniques.

- The data or information is noisy.

- Data labels are not immediately available. Frauds or intrusions usually aware after they have already happened.

- It is hard to track user‟s behaviors. All types of users (good users, business, and fraudsters) change their behaviors frequently

Security Mechanism to Prevent from Fraud

These are the existing security mechanism that helps to prevent from fraudulent transactions:

- **Address Verification Service (AVS)**: In this technique it matches the cardholder billing address and shipping address and identifies whether the cardholder has purchased product on this address. However, this technique contains some weaknesses i.e. the address information is available online; the banker feels boring to check record of every customer to prevent from fraudulent transaction; it cannot check the entire informational card.

- **Fraud Rates:** This technology checks for recognized patterns i.e. used by the fraudster to commit the fraud. The advantage that it is easy to configure and understand, but the disadvantage

- fraudster changes their pattern changes at regular interval.

- **Relocation:** This technology identifies the customer geographic location by identifying its IP addresses.

- **Chip & Pin:** A PIN is a 4 digit unique and secret number that customer has to enter before doing transaction by ATM/Debit Card/Credit Card. The 4 digit pin is used to identify whether the customer is genuine or not.

- **3D-Secure:** This technology works on the principle of authenticating the user password with the password i.e. stored in the database. The main advantage of this system is that fraudster needs a user‟s password to perform the transaction.

- **Biotechnology:** The unique characteristic of each customer such as fingerprints, voice, signature, iris, and other similar biological components is stored in a computer so that a computer can read it. Then the computer compares the stored patterns to the person who is performing the transaction to identify whether the customer is genuine. The main disadvantage of this technology is that is that it requires additional hardware cost.

- **One Time Password:** The random number is generated at server side and is send to the customer‟s mobile phone through the help of the web services to ensure that the correct user is performing the transaction at that instant of time. The user has to enter the same password for getting the authorization from the bank side.

Delimitations of the study

- Selected sample size is only 50 so that is the main concern related to this study
- Due to busy schedule and time constraints. It is not possible to meet personally to all person to get exact data for this research

CHAPTER – IV

ANALYSIS & DISCUSSION

HDFC Bank Limited is an Indian banking and financial services company headquartered in Mumbai. It is India's largest private sector bank by assets and world's 10th largest bank by market capitalisation as of April 2021. It is the third largest company by market capitalisation of $122.50 billion on the Indian stock exchanges. It is also the fifteenth largest employer in India with nearly 150,000 employees.

HDFC Bank was incorporated in 1994 as a subsidiary of the Housing Development Finance Corporation, with its registered office in Mumbai, Maharashtra, India. Its first corporate office and a full-service branch at Sandoz House, Worli were inaugurated by the then Union Finance Minister, Manmohan Singh.

As of 30 June 2022, the bank's distribution network was at 6,378 branches across 3,203 cities. It has installed 430,000 POS terminals and issued 23,570,000 debit cards and 12 million credit cards in FY 2017. It has a base of 1,52,511 permanent employees as of 30 June 2022.

Cyber Frauds

Social Engineering causing majority of cyber frauds, Manish Agrawal, Head – Credit Intelligence and Control, HDFC Bank

HDFC Bank recently concluded its second analysis on cyber frauds in India for the assessment of year 2021 and gave the outlook for 2022. Some of the quick highlights busts few myths about cyber frauds.

A fraud dispute time analysis by HDFC Bank reveals that 65-70 percent of cyber frauds now happen between 7.00 AM and 7.00 PM, contrary to the perception that frauds happen only in the middle of the night.

HDFC Bank‟s study further reveals that 80-85% of the affected customers are in the age group 22-50, who supposedly belonged to the more tech savvy age bracket. It‟s usually presumed that only the elderly get defrauded

70-80 percent or even more of cyber frauds are happening through social engineering tactics, where the modus operandi is through Greed, Threat, Help (GTH) mechanism. “It‟s not about the system vulnerabilities or exploitation but it is always about the social engineering tactics,” says Manish Agrawal, Head Credit Intelligence and Control, HDFC Bank.

A major eye-opener from the analysis is the vulnerability of the young population falling prey to cyber frauds. They are being tricked by social engineering techniques because of not paying enough cognizance to basic hygiene while conducting banking transactions on digital channels.

Fraudsters adopt the GTH formula

The script to defraud the customer is written around Greed, Threat, Help (GTH). The scenarios are built to entice the customer towards making them to believe a false offer and then entrap : “you have won a lottery, prize, etc; we will get a job for you;

matrimonial frauds; gifts lying at the airport awaiting duty payment and clearance, etc." These are all examples of Greed.

The customers are threatened to provide personal details, in the absence of which the bank account will be closed or the card will be blocked / the mobile services will be discontinued, etc.

Finally, „Help". In the corona period, there were instances of calls made to customers who were seeking oxygen cylinders. They are made to pay before the services are provided, which they willingly do because of the dire requirement and then get duped. These are the examples of the citizens being pushed to trap themselves.

The digital transactions also have a pull mechanism whereby the customers self-trap themselves by attracting the fraudsters towards them. For example, people posting a sell advertisement of their vehicles on various digital platforms. The buyer in this case will ask the seller to authenticate the link shared by him (with the UPI PIN) to receive the payment and thus the fraud happens. The reality is that a customer has to never authenticate for receiving money.

Awareness is the key

The digital transaction security awareness should begin at the house level, "Every house should have one evangelist who regularly nudges the family members to follow the hygiene rules while conducting digital transactions," suggests Agrawal.

The HDFC Bank is also running a campaign across the country to make citizens and children aware about how to safely conduct digital transactions. The bank is organizing 2000 secure banking workshops to create awareness about digital frauds.

In fact, as of November 2021, the bank has already covered 99 cities/towns across India through these workshops; 23 of these workshops were conducted in tier II-IV cities; 137 workshops across schools/colleges covering over 10000 students to inculcate early safe banking habits.

Card-on-file (CoF) tokenisation to be introduced from January 2022

The citizens should embrace all the latest digital transaction safety features allowed and facilitated by RBI. The RBI in September 2021 allowed companies to provide Card-on-file (CoF) tokenisation to enhance the security of card transactions.This will come into effect from January 1, 2022.

The CoF tokenisation basically allows customers doing digital transactions to convert their card details into a 16 digit token number, which will prevent the hackers or fraudsters from misusing the data even if it‟s hacked. As it will be difficult for them to decipher the card details from the token number. “At the ecosystem level, the RBI is putting in a lot of controls and i think it‟s phenomenal and the customers should make sure they adopt these measures for securing their digital transactions,” feels Agrawal.

In the case of HDFC Bank‟s card customers, effective January 1, 2022, the HDFC Bank card details saved on merchant website/app will get deleted by the merchants as per the RBI mandate for enhanced card security. To pay each time, the customers will have to enter full card details or opt for tokenisation.

India has one of the highest percentage of real time settlement in the world. This further enhances the need for the country to guard the digital transactions space.

CYBER CRIMES AND FRAUD MANAGEMENT

Technological revolutions both in communication and information technology have changed the way of doing business. In todays changed and changing environment electronic commerce and electronic banking has become an integral part of customers as well as bankers. On account of e-commerce and e- banking distances of locations have reduced and many international financial markets have been linked. While it can be appreciated that the computers have become an integral part of one„s life, it has also created space for cyber crimes. In view of the fast changing world on account of significant contribution of the IT sector, the cyber crimes pose a significant threat. Cyber crimes are usually carried out by the criminals with technical knowledge and can outstrip and think one step ahead to penetrate into the computers to carry out the crimes.

Cyber Crimes A cyber crime can be defined as ―criminal activity carried out by using computers and internet‖. A cyber crime can also be defined as ―use of computers and/ or other electronic devices via information systems like computer network, internet to handle illegal activities like transfer of funds, withdrawal of funds through unauthorized access‖

Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against property, government and people at large. In cyber crimes, computers are either used as tools and/or targets. So the computer which is an electronic devise is used as a medium of cyber crimes. Effects of cyber crimes:

- Financial loss
- Sabotage and theft to identifiable information
- Exposed to reputation risks
- Infringement of confidential information
- Legal consequences
- Operational risks

LEGAL REGIME TO CONTROL BANK FRAUDS

Reasons for cyber crimes

Easy access to data: If a cyber criminal is able to break into a computer,,s system, the access to the sensitive data including customer,,s confidential financial data, information can be copied into a small removable device. Since information technology drives the functioning of corporate, individuals, banks and government departments and other professionals, the storage of unprotected sensitive data and information in their computers pose a significant threat. Negligence on the part of the users: Individuals and the employees, officers, executives and other professionals who use the computer systems should be vigilant to protect their information and sensitive data stored in the computers. They should be very careful while using such devices by protecting the access to the system through proper usage of Personal Identification Number (PIN) and passwords. Any negligence on their part would make the cyber criminals,, access to such devices and information easy Lack of internal control in organizations and banks.

A computer system works based on instructions received from operating systems which are driven by a number of codes. An in-effective internal control and IT audit system would lead to lapses in the computerized environment on account of availability of inefficient hardware systems and software systems. Hence banks should ensure that ongoing internal control and IT audit systems are in place. All software used for operating systems should be audited by an IT auditor and certified about their sensitivity, integrity and security. The operating systems should have clear demarcation of access by users at different levels. Since banks use many operating systems for their daily operations for transfer of funds, maintain customer deposit and loan and other accounts, preparation of regulatory returns, financial statements like balance sheets, P&L accounts and other sensitive information and data, allows Core Banking Solutions, use RTGS,NEFT, ECS etc., there should be an effective control to avoid unauthorized access. Hence, the access to the operating systems should have dual control of access based on authorizations.

Complex: The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

Negligence: Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system.

Loss of evidence: Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

Information Technology Act, 2000 & other Relevant Acts

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000.

This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand what are the various perspectives of the IT Act, 2000 and what it offers.

The Information Technology Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

The Act also provides for the constitution of the Cyber Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act. The said Act also proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

Objectives of I.T. legislation in India It is against this background the Government of India. Enacted its Information Technology Act 2000 with the objectives as follows, stated in the preface to the Act itself. ―to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.‖ The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000, got President assent on 9 June and was made effective from 17 October 2000.

- The Act essentially deals with the following issues:
- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions
- Justice Dispensation Systems for cyber crimes.

Amendment Act 2008 Being the first legislation in the nation on technology, computers and ecommerce and e-communication, the Act was the subject of extensive debates, elaborate reviews and detailed criticisms, with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. There were some conspicuous omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in technology

based cases with the I.T. Act also being referred in the process and the reliance more on IPC rather on the ITA.

Thus the need for an amendment – a detailed one – was felt for the I.T. Act almost from the year 2003-04 itself. Major industry bodies were consulted and advisory groups were formed to go into the perceived lacunae in the I.T. Act and comparing it with similar legislations in other nations and to suggest recommendations. Such recommendations were analysed and subsequently taken up as a comprehensive Amendment Act and after considerable administrative procedures, the consolidated amendment called the Information Technology Amendment Act 2008 was placed in the Parliament and passed without much debate, towards the end of 2008 (by which time the Mumbai terrorist attack of 26 November 2008 had taken place). This Amendment Act got the President assent on 5 Feb 2009 and was made effective from 27 October 2009. Some of the notable features of the ITAA are as follows:

- Focusing on data privacy
- Focusing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognising the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like child pornography and cyber terrorism
- Authorizing an Inspector to investigate cyber offences (as against the DSP earlier)

The Act totally has 13 chapters and 90 sections (the last four sections namely sections 91 to 94 in the ITA 2000 dealt with the amendments to the four Acts namely the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers,, Books Evidence Act

1891 and the Reserve Bank of India Act 1934). The Act begins with preliminary and definitions and from thereon the chapters that follow deal with authentication of electronic records, digital signatures, electronic signatures etc. Elaborate procedures for certifying authorities (for digital certificates as per IT Act -2000 and since replaced by electronic signatures in the ITAA -2008) have been spelt out. The civil offence of data theft and the process of adjudication and appellate procedures have been described. Then the Act goes on to define and describe some of the well-known cyber crimes and lays down the punishments therefore. Then the concept of due diligence, role of intermediaries and some miscellaneous provisions have been described

Applicability (Inclusions and exclusions) The Act extends to the whole of India and except as otherwise provided, it applies to also any offence or contravention there under committed outside India by any person. There are some specific exclusions to the Act (i.e. where it is not applicable) as detailed in the First Schedule, stated below:

i) negotiable instrument (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;

ii) a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;

iii) a trust as defined in section 3 of the Indian Trusts Act, 1882

iv) a will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition

v) any contract for the sale or conveyance of immovable property or any interest in such property;

vi) any such class of documents or transactions as may be notified by the Central Government Sections and penalties

Section 43 deals with penalties and compensation for damage to computer, computer system etc. This section is the first major and significant legislative step in India to combat the issue of data theft.

The IT industry has for long been clamouring for legislation in India to address the crime of data theft, just like physical theft or larceny of goods and commodities. This Section addresses the civil offence of theft of data. If any person without permission of the owner or any other person who is in charge of a computer, accesses or downloads, copies or extracts any data or introduces any computer contaminant like virus or damages or disrupts any computer or denies access to a computer to an authorised user or tampers etc…he shall be liable to pay damages to the person so affected. Earlier in the ITA -2000 the maximum damages under this head was Rs.1 crore, which (the ceiling) was since removed in the ITAA 2008.

The essence of this Section is civil liability. Criminality in the offence of data theft is being separately dealt with later under Sections 65 and 66. Writing a virus program or spreading a virus mail, a bot, a Trojan or any other malware in a computer network or causing a Denial of Service Attack in a server will all come under this Section and attract civil liability by way of compensation. Under this Section, words like Computer Virus, Compute Contaminant, Computer database and Source Code are all described and defined. Questions like the employees,, liability in an organisation which is sued against for data theft or such offences and the amount of responsibility of the employer or the owner and the concept of due diligence were all debated in the first few years of ITA -2000 in court litigations like the bazee.com case and other cases. Subsequently need was felt for defining the corporate liability for data protection and information security at the corporate level was given a serious look.

Thus the new Section 43-A dealing with compensation for failure to protect data was introduced in the ITAA -2008. This is another watershed in the area of data protection especially at the corporate level. As per this Section, where a body corporate is negligent in implementing reasonable security practices and thereby causes wrongful loss or gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected. The Section further explains the phrase body corporate,, and quite significantly the phrases reasonable security practices and procedures,, and sensitive personal data or information,,.

Thus the corporate responsibility for data protection is greatly emphasized by inserting Section 43A whereby corporate are under an obligation to ensure adoption of reasonable security practices. Further what is sensitive personal data has since been clarified by the central government vide its Notification dated 11 April 2011 giving the list of all such data which includes password, details of bank accounts or card details, medical records etc. After this notification, the IT industry in the nation including tech savvy and widely technology-based banking and other sectors became suddenly aware of the responsibility of data protection and a general awareness increased on what is data privacy and what is the role of top management and the Information Security Department in organisations in ensuring data protection, especially while handling the customers,, and other third party data.

- Reasonable Security Practices
- Site certification
- Security initiatives
- Awareness Training
- Conformance to Standards, certification
- Policies and adherence to policies
- Policies like password policy, Access
- Control, email Policy etc
- Periodic monitoring and review.

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules have since been notified by the Government of India, Dept of I.T. on 11 April 2011. Anybody corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies

containing managerial, technical, operational and physical security control measures commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.

The international Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub-rule (1). In view of the foregoing, it has now become a major compliance issue on the part of not only IT companies but also those in the Banking and Financial Sector especially those banks with huge computerised operations dealing with public data and depending heavily on technology. In times of a litigation or any security breach resulting in a claim of compensation of financial loss amount or damages, it would be the huge responsibility on the part of those body corporate to prove that that said ―Reasonable Security Practices and Procedures‖ were actually in place and all the steps mentioned in the Rules passed in April 2011 stated above, have been taken.

Adjudication Having dealt with civil offences, the Act then goes on to describe civil remedy to such offences in the form of adjudication without having to resort to the procedure of filing a complaint with the police or other investigating agencies. Adjudication powers and procedures have been elaborately laid down in Sections 46 and thereafter. The Central Government may appoint any officer not below the rank of a director to the Government of India or a state Government as the adjudicator. The I.T. Secretary in any state is normally the nominated Adjudicator for all civil offences arising out of data thefts and resultant losses in the particular state. If at all one section can be criticized to be absolutely lacking in popularity in the IT Act, it is this provision. In the first ten years of existence of the ITA, there have been only a very few applications made in the nation, that too in the major metros almost all of which are under different stages of judicial process and adjudications have been obtained in possibly less than five cases. The first adjudication obtained under this provision was in Chennai, Tamil Nadu, in a case involving ICICI Bank in which the bank was told to compensate the applicant with

the amount wrongfully debited in Internet Banking, along with cost and damages. in April 2010. This section should be given much popularity and awareness should be spread among the public especially the victims of cyber crimes and data theft that such a procedure does exist without recourse to going to the police and filing a case. It is time the state spends some time and thought in enhancing awareness on the provision of adjudication for civil offences in cyber litigations like data theft etc so that the purpose for which such useful provisions have been made, are effectively utilized by the litigant public.

ADVANTAGE OF CYBER LAWS

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.

From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects.

- Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.

- Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.

- Digital signatures have been given legal validity and sanction in the Act.

- The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.

- The Act now allows Government to issue notification on the web thus heralding e-governance.

Other Banking Related Laws

Limitation Act – Important Aspects

The Limitation Act, 1963 specifies certain period prescribed within which any suit appeal or application can be made. The ‗prescribed period,, means the period of limitation computed in accordance with the provisions of the Limitation Act. A banker is allowed to take legal action by filing a suit, prefer an appeal and apply for recovery only when the documents are within the period of limitation. On the other hand, if the documents expired or are time barred, the banker cannot take any legal course of action to recover the dues. Therefore, banks should be careful to ensure that all legal loan documents held are valid and not time barred. In other words, it is the responsibility of lenders to ensure that all loan documents are properly executed and they are all within the required limitation period as per the limitation act. This is one of the crucial aspect in credit management of banks.

THE CONSUMER PROTECTION ACT, 1860

To protect the interests of the consumers, the Consumer Protection Act was enacted. The Act extends to the whole of India except the State of Jammu and Kashmir. The Act covers all goods and services, except goods for resale or for commercial purpose and services rendered free of charge and a contract of personal service. Complaints (i.e., any allegation should be in writing made by a complainant to obtain any relief provided by or under this Act) The complaint may be made by the complainant which includes a consumer or any voluntary consumer association registered under the Companies Act 1956 or any other law or the Central or State Government or one or more consumers, having the same interest and in case of death of a consumer his/ her legal heirs or

representative. The Act is for speedy disposal of the redressal of consumer disputes. Consumer councils are established to promote and protect the rights of consumers. The Central Council has the jurisdiction for the entire country, followed by the State Council for each state and District Council for each district. The Councils at the State level is headed by the chairman of the council, i.e., the Minister-in-Charge of the Consumer Affairs in the State Government. The consumers,, complaints are dealt by District Forum, State and National Commission. District forum and State Commission are established by the State Governments, and the National Commission established by Central Government. District Forum has powers to deal with cases up to 20 lakhs. The State Commission deals with complaints exceeding value of 20 lakh and below One crore and appeals against the orders of any District forum within the State. The cases exceeding One crore would be handled by the Central Commission. They also deal with appeals against the order of any State Commission. Complaints should be in a prescribed manner, with full details, evidence and applicable fee. Supporting affidavit is required. Admissibility of complaint is to be decided within twenty one days.

THE INDIAN PENAL CODE, 1860

The Indian Penal Code (IPC) is the main criminal code of India. It is a comprehensive code intended to cover all substantive aspects of criminal law. The code was drafted in 1860 on the recommendations of first law commission of India established in 1834 under the Government of India Act 1833 under the Chairmanship of Thomas Babington Macaulay. It came into force in British India during the early British Raj period in 1862. However, it did not apply automatically in the Princely states, which had their own courts and legal systems until the 1940s. The Code has since been amended several times and is now supplemented by other criminal provisions. Based on IPC, Jammu and Kashmir has enacted a separate code known as Ranbir Penal Code (RPC).

After the partition of the British Indian Empire, the Indian Penal Code was inherited by its successor states, the Dominion of India and the Dominion of Pakistan, where it continues independently as the Pakistan Penal Code. After the independence of Bangladesh from Pakistan, the code continued in force there. The Code was also adopted by the British colonial authorities in Colonial Burma, Ceylon (modern Sri Lanka), the

Straits Settlements (now part of Malaysia), Singapore and Brunei, and remains the basis of the criminal codes in those countries. The Ranbir Penal Code applicable in Jammu and Kashmir is also based on this Code

THE INDIAN EVIDENCE ACT 1872

The Indian Evidence Act, identified as Act no. 1 of 1872, and called the Indian Evidence Act, 1872, has eleven chapters and 167 sections, and came into force 1 September 1872. At that time, India was a part of the British Empire. Over a period of more than 125 years since its enactment, the Indian Evidence Act has basically retained its original form except certain amendments from time to time.

When India gained independence on 15 August 1947, the Act continued to be in force throughout the Republic of India and Pakistan, except the state of Jammu and Kashmir. Then, the Act continues in force in India, but it was repealed in Pakistan in 1984 by the Evidence Order 1984 (also known as the "Qanun-e-Shahadat"). It also applies to all judicial proceedings in the court, including the court martial. However, it does not apply on affidavits and arbitration. Some important section is;

Sec.32 - Statement by person who is dead or cannot be found.

Sec.45- Opinion of experts.

Sec.46 - Facts bearing upon opinions of experts.

Sec.51- Grounds of opinion when relevant.

Sec.57- Facts of which court must take judicial notice.

Sec.58- Fact admitted need not be proved

Sec.60- Oral evidence must be direct.

Sec.73- Comparison of signature, writing a seal.7

This Act is divided into three parts and there are 11 chapters in total under this Act.

1. Cheating (Section 415, IPC)

Remedial Measures: The preventive measures in respect of the cheating can be concentrated on cross-checking regarding identity, genuineness, verification of particulars, etc. in respect of various instruments as well as persons involved in encashment or dealing with the property of the bank.

2. Criminal misappropriation of property (Section 403 IPC).

Remedial Measure : Criminal misappropriation of property, presuppose the custody or control of funds or property, so subjected, with that of the person committing such frauds. Preventive measures, for this class of fraud should be taken at the level the custody or control of the funds or property of the bank generally vests. Such a measure should be sufficient, it is extended to these persons who are actually handling or having actual custody or control of the fund or movable properties of the bank.

3. Criminal breach of trust (Section 405, IPC)

Remedial Measure : Care should be taken from the initial step when a person comes to the bank. Care needs to be taken at the time of recruitment in bank as well.

4. Forgery (Section 463, IPC)

Remedial Measure: Both the prevention and detection of frauds through forgery are important for a bank. Forgery of signatures is the most frequent fraud in banking business. The bank should take special care when the instrument has been presented either bearer or order; in case a bank pays forged instrument he would be liable for the loss to the genuine costumer.

5. Falsification of accounts (Section 477A)

Remedial Measure: Proper diligence is required while filling of forms and accounts. The accounts should be rechecked on daily basis.

6. Theft (Section 378, IPC)

Remedial Measures : Encashment of stolen' cheque can be prevented if the bank clearly specify the age, sex and two visible identify action marks on the body of the person traveler's cheques on the back of the cheque leaf. This will help the paying bank to easily identify the cheque holder.

Theft from lockers and safe deposit vaults are not easy to commit because the master-key remains with the banker and the individual key of the locker is handed over to the costumer with due acknowledgement.

7. Criminal conspiracy (Section 120 A, IPC)

In the case of State of Andhra Pradesh v. IBS Prasad Rao and Other, the accused, who were clerks in a cooperative Central Bank were all convicted of the offences of cheating under Section 420 read along with Section 120 A. all the four accused had conspired together to defraud the bank by making false demand drafts and receipt vouchers.

8. Offences relating to currency notes and banks notes (Section 489 A-489E, IPC)

These sections provide for the protection of currency-notes and bank notes from forgery. The offences under section are:

(i) Counterfeiting currency notes or banks.

(ii) Selling, buying or using as genuine, forged or counterfeit currency notes or bank notes. Knowing the same to be forged or counterfeit.

(iii) Possession of forged or counterfeit currency notes or bank-notes, knowing or counterfeit and intending to use the same as genuine.

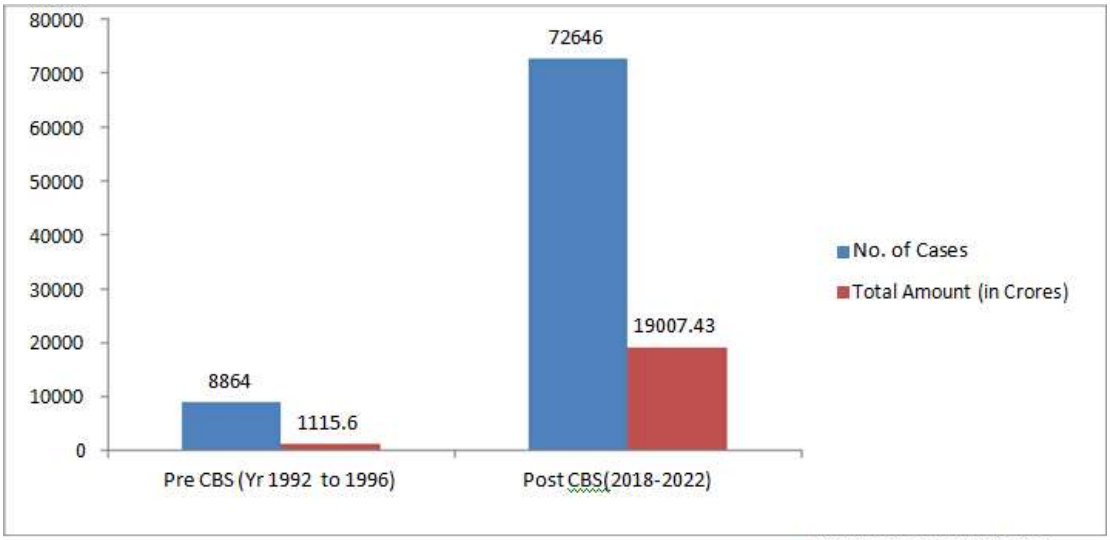
(iv) Making or passing instruments or materials for forging or counterfeiting currency notes or banks.

(v) Making or using documents resembling currency-notes or bank notes. Most of the above provisions are Cognizable Offences under Section 2(c) of the Code of Criminal Procedure, 1973.

Legislations in other nations

As against the lone legislation ITA and ITAA in India, in many other nations globally, there are many legislations governing e-commerce and cyber crimes going into all the facets of cyber crimes. Data Communication, storage, child pornography, electronic records and data privacy have all been addressed in separate Acts and Rules giving thrust in the particular area focused in the Act. In the US, they have the Health Insurance Portability and Accountability Act popularly known as HIPAA which inter alia, regulates all health and insurance related records, their upkeep and maintenance and the issues of privacy and confidentiality involved in such records. Companies dealing with US firms ensure HIPAA compliance insofar as the data relating to such corporate are handled by them. The Sarbanes-Oxley Act (SOX) signed into law in 2002 and named after its authors Senator Paul Sarbanes and Representative Paul Oxley, mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud. Besides, there are a number of laws in the US both at the federal level and at different states level like the Cable Communications Policy Act, Children„s Internet Protection Act, Children„s Online Privacy Protection Act etc. In the UK, the Data Protection Act and the Privacy and Electronic Communications Regulations etc are all regulatory legislations already existing in the area of information security and cyber crime prevention, besides cyber crime law passed recently in August 2011. Similarly, we have cyber crime legislations and other rules and regulations in other nations.

Data collection and analysis related to cyber crime in Banking in India



Source: Based on RBI Data

The above data and trends were collected from different sources, one from reserve bank of India website and it was compared with the data collected from one book. The data clearly shows that post CBS implementation, number of cases and amount involved in such cases has gone up substantially in comparison to pre CBS implemenation .

The first RTI was filled to RBI on 20th July 2016. RBI was asked to provide the depth information. Cyber Frauds Nos. Type wise for ICICI Bank, Axis Bank, HDFC Bank, HSBC Bank, Citi Bank, State Bank of India, Punjab National Bank, Bank of Baroda, IDBI Bank, Indian Bank for the year wise, Bank wise and type of frauds wise.

Frauds related to credits cards, ATM/Debit cards& Internet Banking are clear with the help of this chart

Bank Name	Type of fraud	2021-22	2020-21	2019-20	2018-19	2017-18
Allahabad Bank	Credits Cards	1	0	0	0	0
	ATM/Debit cards	0	0	1	0	0
American Express Banking Corp.	Credits Cards	108	137	218	166	153
	Internet Banking	1	0	0	0	0
Andhra Bank	Credits Cards	0	0	0	1	0
	Internet Banking	0	1	0	0	0

Axis Bank Ltd.	Credits Cards	9	13	9	13	49
	ATM/Debit cards	9	13	7	27	37
	Internet Banking	12	28	28	6	0
Bank of Baroda	ATM/Debit cards	3	1	0	1	13
	Internet Banking	0	0	0	3	0
Bank of India	Credits Cards	2	2	2	0	1
	ATM/Debit cards	2	1	0	1	1
	Internet Banking	0	1	0	0	2
Bank of Maharashtra	ATM/Debit cards	0	0	1	1	0
	Internet Banking	1	1	3	0	1
Barclays Bank Plc	Credits Cards	1	0	0	0	0
Canara Bank	Credits Cards	0	0	1	0	0
	ATM/Debit cards	0	1	0	0	0
	Internet Banking	0	1	0	0	0
Central bank of India	Credits Cards	0	1	2	4	9
	ATM/Debit cards	0	0	18	2	2
Citi Bank N.A.	Credits Cards	104	123	64	62	81
	ATM/Debit cards	15	10	17	13	25
	Internet Banking	3	3	1	0	0
Corporation Bank	Credits Cards	0	2	7	0	6
	ATM/Debit cards	0	4	6	3	1
	Internet Banking	2	1	1	0	1
Dena Bank	Credits cards	0	0	0	1	0
Deutsche Bank (Asia)	Credits Cards	4	0	0	0	0
	ATM/Debit cards	1	0	1	1	1
	Internet Banking	0	0	0	1	0
Dhanlaxmi Bank ltd.	Credits cards	1	0	0	0	0
	Internet Banking	0	0	0	1	0
Federal Bank Ltd.	ATM/Debit cards	0	1	0	0	0
	Internet Banking	0	0	0	1	0

HDFC Bank Ltd.	Credits Cards	37	108	61	105	94
	ATM/Debit cards	20	24	39	47	69
	Internet Banking	0	0	0	0	1
Hongkong& Shanghai Banking Corporation Ltd.	Credits Cards	24	27	66	21	24
	ATM/Debit cards	4	7	13	11	11
ICICI Bank Ltd.	Credits Cards	83	94	124	101	77
	ATM/Debit cards	34	18	55	119	263
	Internet Banking	55	29	88	2	0
IDBI Bank Limited	ATM/Debit cards	0	1	2	1	52
	Internet Banking	5	16	0	2	0
Indian Bank	ATM/Debit cards	0	0	0	3	3
	Internet Banking	0	3	0	3	0
Indian Overseas Bank	Credits Cards	0	0	0	1	0
	ATM/Debit cards	1	0	0	0	0
Induslnd Bank Ltd.	Credits Cards	0	2	2	2	3
	ATM/Debit cards	0	0	1	0	1
	Internet Banking	0	0	6	1	0
ING Vysya Bank Ltd.	ATM/Debit cards	0	0	1	0	0
Jammu & Kashmir Bank Ltd.	Credits Cards	0	1	1	1	0

Karnataka Bank Ltd.	ATM/Debit cards	0	0	0	1	0
	Internet Banking	0	0	5	2	0
Kotak Mahindra Bank Ltd.	Credits Cards	5	7	7	4	11
	ATM/Debit cards	0	1	2	9	30
	Internet Banking	9	7	15	3	11
Shinhan Bank	ATM/Debit cards	0	0	0	0	1
Lakshmi Vilas Bank Ltd.	ATM/Debit cards	0	0	0	0	1
	Internet Banking	0	1	0	0	0
Oriental Bank of Commerce	ATM/Debit cards	0	0	0	0	4
	Internet Banking	0	0	0	0	1
Punjab National Bank	Credits Cards	1	0	1	0	1
	ATM/Debit cards	0	2	0	0	2
	Internet Banking	10	1	10	0	0
RBL Bank Ltd.	Credits Cards	0	0	0	9	5
	ATM/Debit cards	0	0	0	1	0

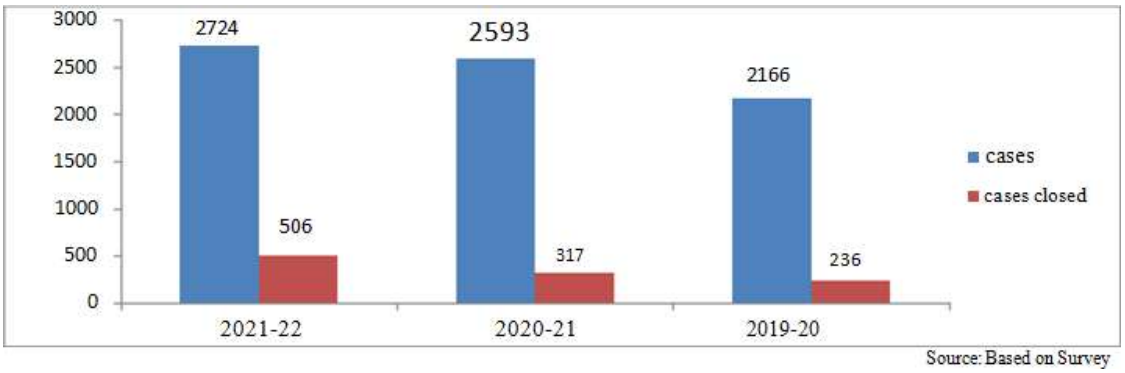
	Internet Banking	0	0	1	1	1
South Indian Bank Ltd.	ATM/Debit cards	0	0	0	1	0
Standard Chartered Bank	Credits Cards	34	52	63	52	101
	ATM/Debit cards	1	10	14	16	21
	Internet Banking	0	0	0	1	0
State Bank of Bikaner & Jaipur	ATM/Debit cards	0	1	0	0	0
State Bank of	ATM/Debit cards	2	8	0	0	0

Hyderabad						
State Bank of India	ATM/Debit cards	0	0	1	1	5
	Internet Banking	2	0	0	1	0
State Bank of Patiala	ATM/Debit cards	2	1	0	0	0
	Internet Banking	0	1	0	0	0
State Bank of Travancore	ATM/Debit cards	2	1	0	1	0
Syndicate Bank	ATM/Debit cards	0	0	0	0	8
	Internet Banking	0	1	0	0	1
Tamilnad Mercantile Bank Ltd.	ATM/Debit cards	0	1	1	0	0
	Internet Banking	0	0	0	1	1
The Royal Bank of Scotland N.V.	Credits Cards	10	8	5	0	0
	ATM/Debit cards	3	1	0	2	4
	Internet Banking	1	0	4	0	2
UCO Bank	ATM/Debit cards	1	2	0	0	0
Union Bank of India	ATM/Debit cards	3	2	1	3	6
	Internet Banking	0	3	1	1	0
United Bank of India	ATM/Debit cards	3	3	0	0	0
	Internet Banking	0	1	0	0	0
Vijaya Bank	Credits Cards	0	1	0	2	0
Yes Bank Ltd.	ATM/Debit cards	0	0	1	1	0
	Internet Banking	0	0	0	2	0

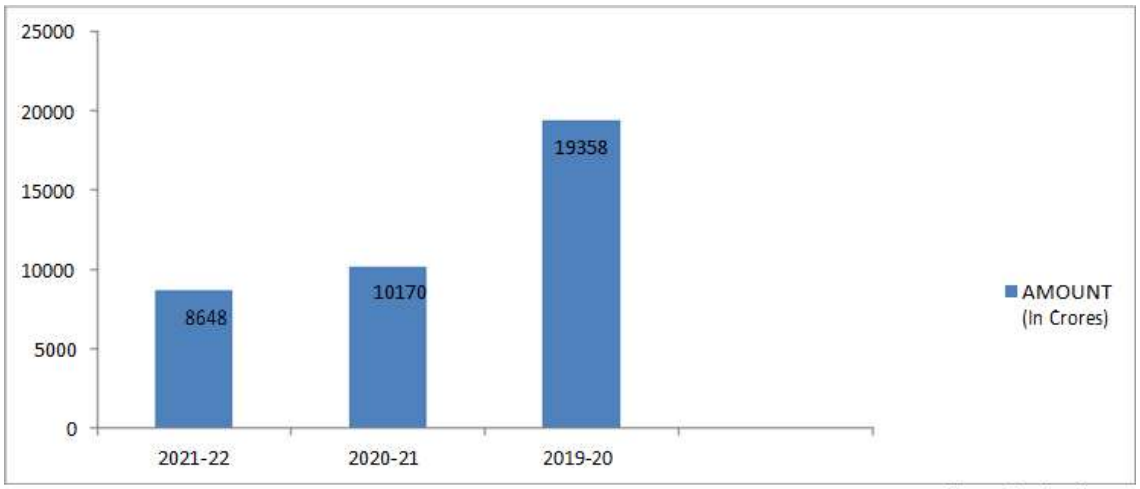
Note : This table represented as per the survey. During the survey researcher found that apart from hdfc bank they also uses other bank services, so researcher also involved another bank data for the survey.

With the help of this chart, it is clear that The American Express Banking corp. Bank has more credits cards frauds in comparison to other banks. These are increasing year by year. On the Other hand, if we see Internet Banking frauds, Axis Bank Ltd. has more frauds in comparison to Others banks. The data shows that the internet banking frauds are increasing in Axis bank. ICICI Bank Ltd. has more ATM frauds in comparisons to other banks and these are increasing year by year. The data clearly shows that the Cyber Frauds are more active.

Private Banks than the Public sector Banks. The data w.r.t. (with respect to) numbers of frauds where the amount involved more than Rs. One Lakh was available at website when the data was searched through different sources like RBI, online search, different newspapers and magazines. The data was found atwebsitewww.indiaspend.com. The data was observed useful so the data is used for the research.



Source: Based on Survey



Source: Based on Survey

The amount involved in bank fraud rose from Rs 10,170 crore ($1.6 billion) in the fiscal year 2020-21 to Rs 19,358crore ($3 billion) in 2019-20, i.e. nearly 100%.

	2021-22		***2020-21***		***2019-20***	
Bank	***No.of frauds reported***	***Extent of loss***	***No.of frauds reported***	***Extent of loss***	***No.of frauds reported***	***Extent of loss***
			PRIVATE SECTOR BANKS			
ICICI Bank Ltd.	*141*	*183.9*	*267*	*273.16*	*222*	*349.79*
HDFC Bank Ltd.	*132*	*224.36*	*100*	*222.27*	*152*	*277.64*
Yes Bank Ltd.	*0*	*0*	*1*	*1.43*	*1*	*19.5*
Axis Bank Ltd.	*54*	*90.67*	*44*	*37.48*	*46*	*26.5*
Federal Bank Ltd.	*1*	*83.35*	*0*	*0*	*1*	*0*

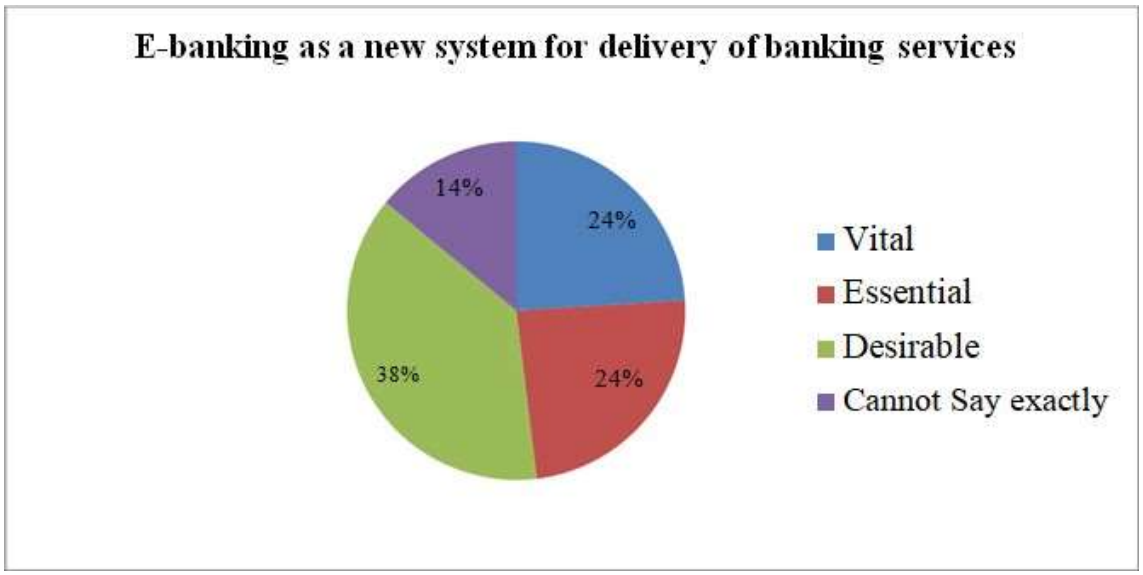
During this research found that the amount lost in cyber frauds and nos. of cases of cyber frauds are much higher in Private sector banks and other bank than the public sector banks. It is anticipated that the internet banking users and mobile banking users may be more with private sector and other banks than the public sector banks and that even reach of these banks may be another reason as Private sector banks and other banks are more popular in Urban areas while public sector banks might be more popular in Rural areas so

to further to investigate the exact reason, the data is enquired from RBI w.r.t. no. of internet banking and mobile banking users with these banks discussed above at Rural and Urban areas.RBI has responded the query and informed that no such data is available with RBI.

RBI website was searched with respect to other information like transactions by ATM cards on different ATM machines, transactions made by credit cards, NEFT transactions and etc. A comparative study based on these data was done for public sector banks, private sector banks and other banks. The transactions are made on ATM and POS.

E- Banking as a new system of delivery banking services:-

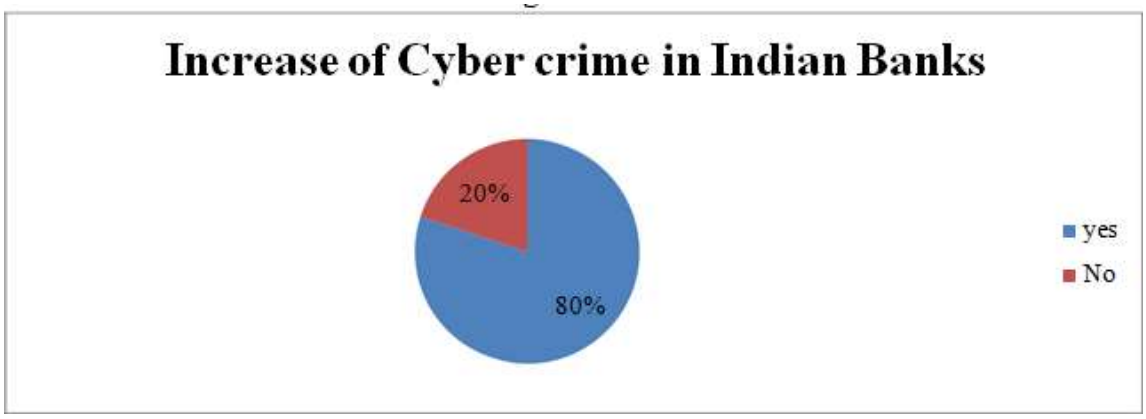
Particular	*Percentage*
Vital	*24%*
Essential	*24%*
Desirable	*38%*
Cannot Say exactly	*14%*



E-banking is a new and very important system of banking services. Now days in digital world, whole banking system depends on it. Above showing response on e-banking services, 24% of total respondents say it is vital, 24% of total respondents are say it is essential, 38% are saying it is desirable, rest 14% can,,t give exactly answer.

Is there is increasing trend in cyber-crime in Indian banking:-

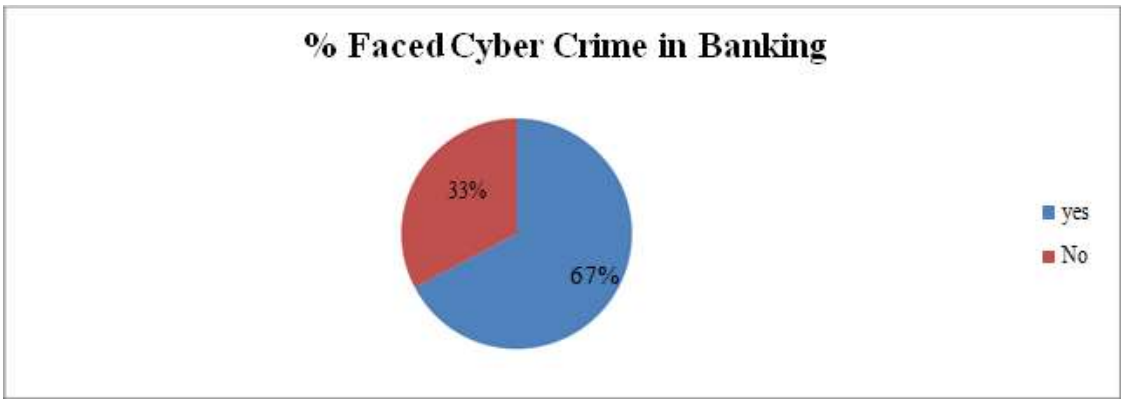
Particular	*Percentage*
Yes	*80%*
No	*20%*



In Indian banking cyber-crime is on increasing trend. According to the survey 80% respondents are agreed with this statement and rest 20% are not agreeing with the fact, it is clear

Have you ever faced cyber-crime related to Banking:-

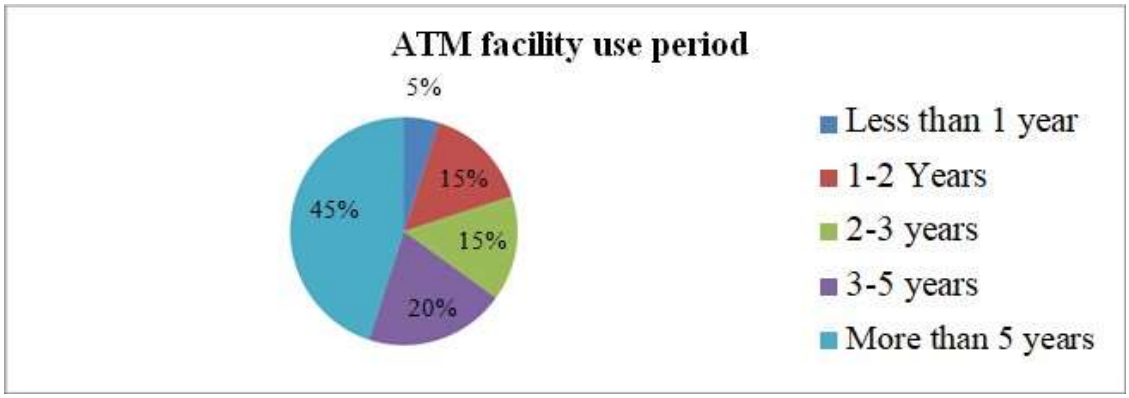
Particular	***Percentage***
Yes	*74%*
No	*36%*



When respondents were asked for whether they have faced any cyber crime then more than 2/3rd respondents have faced the issue, the data shows that 67% respondents have faced such incident and rest 33% have not faced such issue.

How long have you been using ATM facility:-

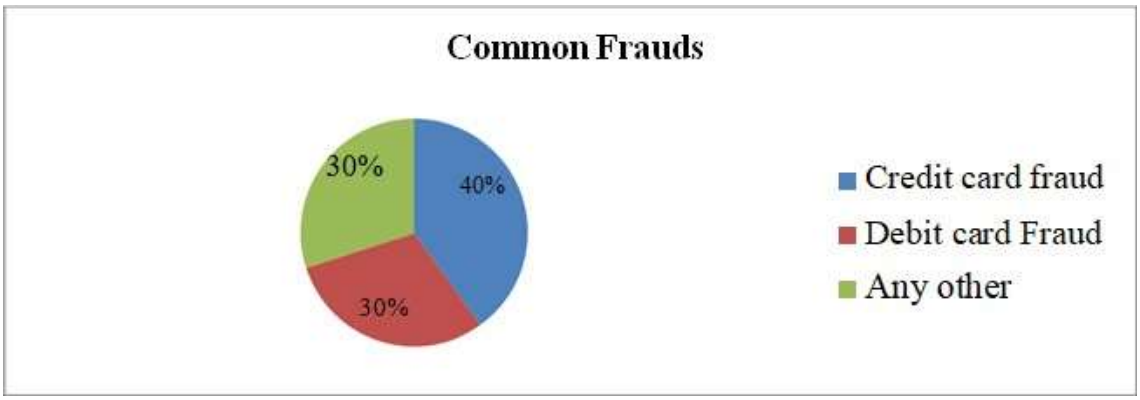
Particular	***Percentage***
Less than 1 year	*4%*
1-2 Years	*16%*
2-3 years	*16%*
3-5 years	*24%*
More than 5 years	*40%*



ATM facility is more popular in all over the world now a days, when this question is asked to the respondents the response was as follows - 4% are using from less than one year, 16% are using 1-2 years, 16% are using 2-3 years, 24% are using 3-5 years, & 40% are using more than five years, it is clearly shown

What kind of fraud is most common:-

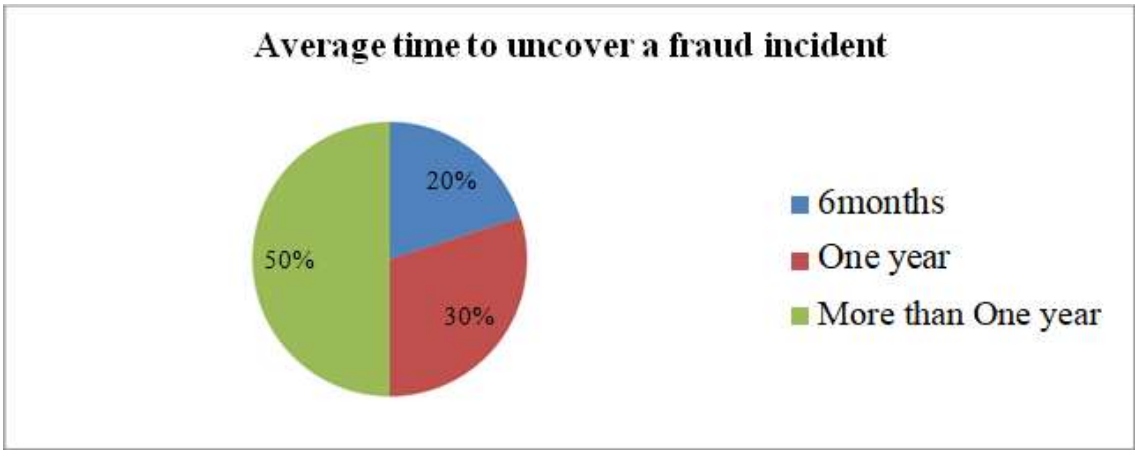
Particular	***Percentage***
Credit card fraud	*40%*
Debit card Fraud	*30%*
Any other	*30%*



When respondents were asked for the type of fraud which is most common, the more prominent type of fraud was observed fraud related to credit cards and the data shows that 40% of respondents informed that credit card fraud is most common, 30% are saying debit card fraud is most common and 30% are saying any other. Banks frauds are increasing day by day. Frauds are causing loss to the victim directly or in directly.

What is in general an average time to uncover a fraud incident:-

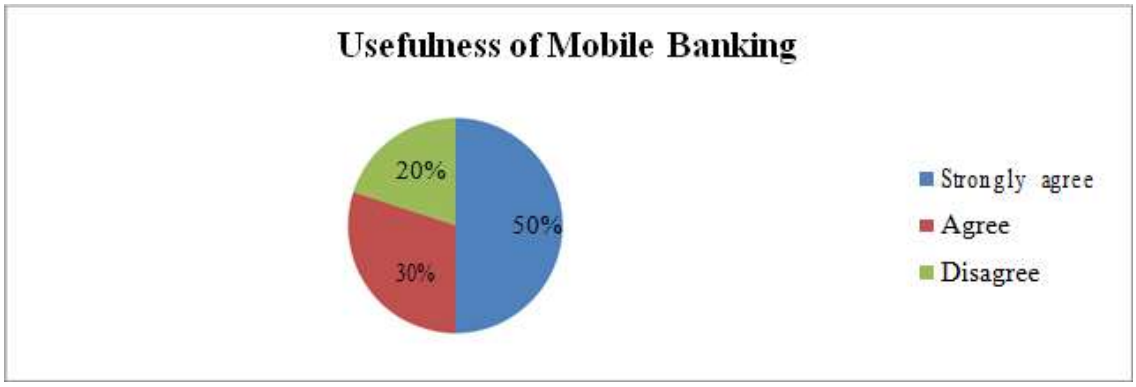
Particular	*Percentage*
6 months	*20%*
One year	*30%*
More than One year	*50%*



It is very typical process to uncover a fraud incident in a very short period. According to the survey that shown in table & figure, 20% of the respondents say average time to uncover a fraud incident is 6 months, 30% are saying average time to uncover a fraud incident is one year and rest 50% are saying it,,s more than one year.

Mobile banking is useful for electronic channel:-

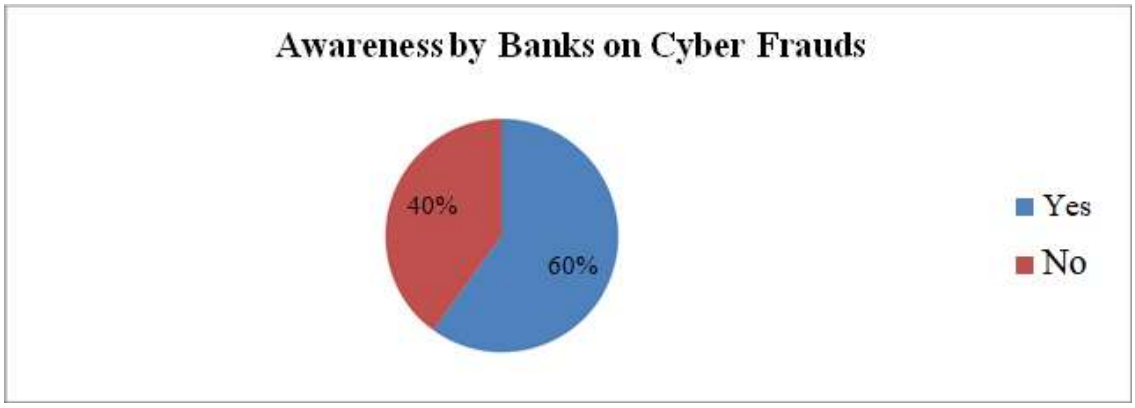
Particular	***Percentage***
Strongly agree	*50%*
Agree	*30%*
Disagree	*20%*



Mobile banking is very important now days, customers don,,t want to go to bank due to less time available because of their daily routine work. All facilities are available in their mobile. With the help of Table and figure, it is clear 50% of the respondents are strongly agree mobile banking is useful, 30% are agree, and rest 20% are disagree with the fact that mobile banking is useful.

Banks provide awareness on frauds

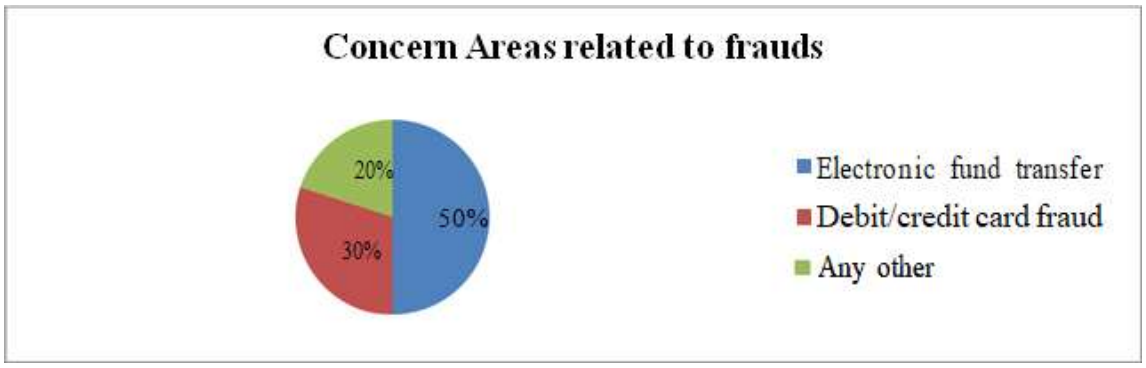
Particular	*Percentage*
Yes	*60%*
No	*40%*



It is very true that banks provide awareness on frauds, because every bank wants to secure their customer at each and every step. In table and figure, 60% of respondents are agreed with the fact that awareness by banks on Cyber Frauds are being provided but 40% are not agreed.

In next two years, which frauds trends will be the area of concern:-

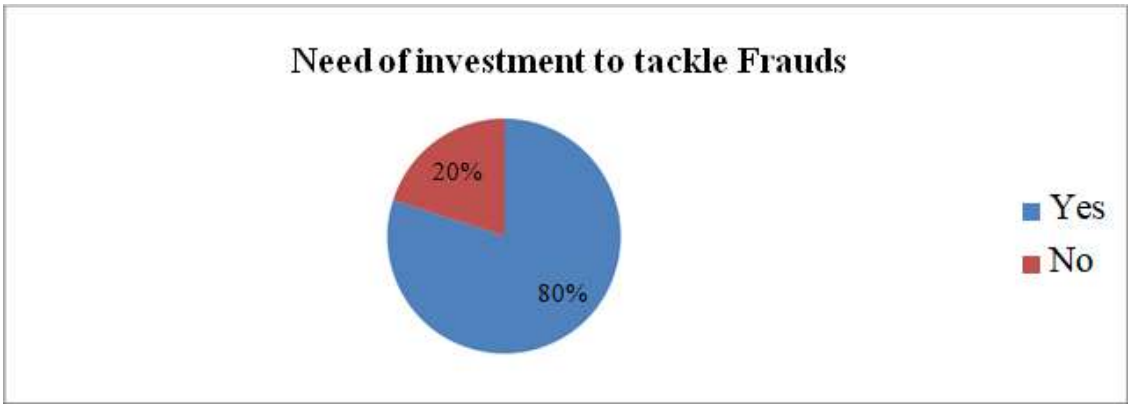
Particular	***Percentage***
Electronic fund transfer	*50%*
Debit/credit card fraud	*30%*
Any other	*20%*



In the table and figure, 50% of the respondents are saying electronic fund transfer is going to be most important fraud in next two years, 30% are saying debit/credit card fraud will be the area of concern, 20% respondents any other frauds are area of concern.

Do banks require more Investment to tackle such frauds:-

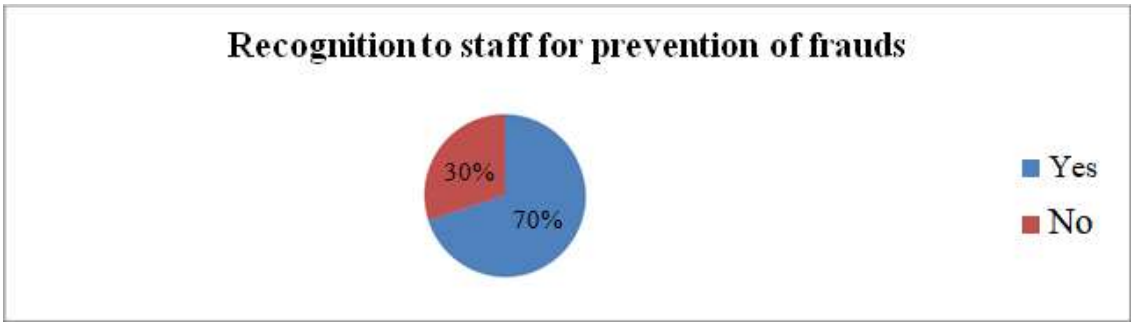
Particular	*Percentage*
Yes	*80%*
No	*20%*



To tackle frauds banks need more investment and also to tackle these frauds banks need to appoint experts. The data shows in table and figure that 80% of respondents are saying bank need more investment and rest 20% are saying that more investment is not required.

Do you want that bank have to give recognition to the staff that prevents frauds in your bank:-

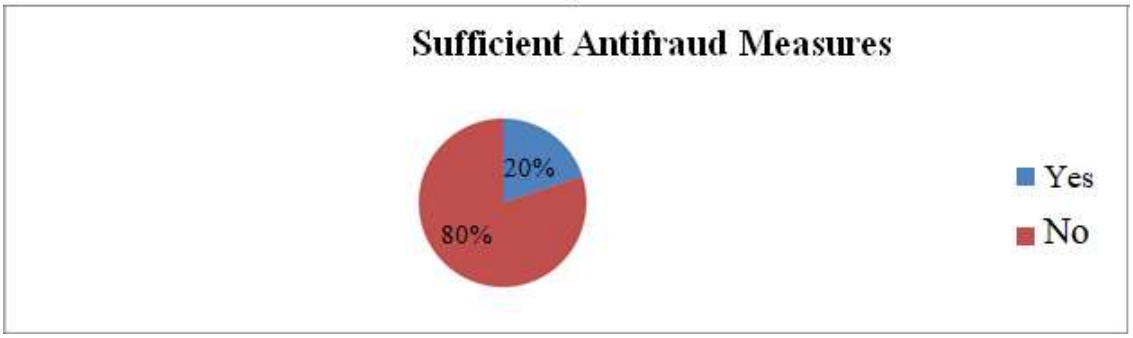
Particular	*Percentage*
Yes	*70%*
No	*30%*



Recognition is must to encourage each age group and specifically to tackle or prevent bank frauds; bank must need to give recognition to their staff to motivate them. In the table and in figure, 70% of the respondents agree that bank should give recognition and 30% are not agreeing. These 30% respondents feel that it is their job responsibilities so why there is a need to give recognition.

Does the available antifraud measures is sufficient:-

Particular	*Percentage*
Yes	*20%*
No	*80%*



In the table and figure, 20% of the respondents are saying they are sufficient antifraud measures and 80% respondents feel that banks need more antifraud measures and it goes with the fact that if antifraud measures are enough then there shall be lesser number of frauds than the current trend.

DATA MINING TECHNIQUES IN FRAUD DETECTION

Fraud that involves cell phones, insurance claims, tax return claims, credit card transactions, government procurement etc. represent significant problems for governments and businesses and specialized analysis techniques for discovering fraud using them are required. These methods exist in the areas of Knowledge Discovery in Databases (KDD), Data Mining, Machine Learning and Statistics. They offer applicable and successful solutions in different areas of electronic fraud crimes.

In general, the primary reason to use data analytics techniques is to tackle fraud since many internal control systems have serious weaknesses. For example, the currently prevailing approach employed by many law enforcement agencies to detect companies involved in potential cases of fraud consists in receiving circumstantial evidence or complaints from whistleblowers. As a result, a large number of fraud cases remain undetected and unprosecuted. In order to effectively test, detect, validate, correct error and monitor control systems against fraudulent activities, businesses entities and organizations rely on specialized data analytics techniques such as data mining, data matching, sounds like function, Regression analysis, Clustering analysis and Gap. Techniques used for fraud detection fall into two primary classes: statistical techniques and artificial intelligence.

Statistical techniques

Data preprocessing techniques for detection, validation, error correction, and filling up of missing or incorrect data.

Calculation of various statistical parameters such as averages, quantiles, performance metrics, probability distributions, and so on. For example, the averages may include average length of call, average number of calls per month and average delays in bill payment.

Models and probability distributions of various business activities either in terms of various parameters or probability distributions.

Computing user profiles.

Time-series analysis of time-dependent data.

Clustering and classification to find patterns and associations among groups of data.

Data matching Data matching is used to compare two sets of collected data. The process can be performed based on algorithms or programmed loops. Trying to match sets of data against each other or comparing complex data types. Data matching is used to remove duplicate records and identify links between two data sets for marketing, security or other uses.

Sounds like Function is used to find values that sound similar. The Phonetic similarity is one way to locate possible duplicate values, or inconsistent spelling in manually entered data. The „sounds like‟ function converts the comparison strings to four-character American Soundex codes, which are based on the first letter, and the first three consonants after the first letter, in each string.

Regression analysis allows you to examine the relationship between two or more variables of interest. Regression analysis estimates relationships between independent variables and a dependent variable. This method can be used to help understand and identify relationships among variables and predict actual results.

Gap analysis is used to determine whether business requirements are being met, if not, what are the steps that should be taken to meet successfully.

Matching algorithms to detect anomalies in the behavior of transactions or users as compared to previously known models and profiles. Techniques are also needed to eliminate false alarms, estimate risks, and predict future of current transactions or users.

Some forensic accountants specialize in forensic analytics which is the procurement and analysis of electronic data to reconstruct, detect, or otherwise support a claim of financial fraud. The main steps in forensic analytics are data collection, data preparation, data analysis, and reporting. For example, forensic analytics may be used to review an

employee's purchasing card activity to assess whether any of the purchases were diverted or divertible for personal use.

Artificial intelligence

Fraud detection is a knowledge-intensive activity. The main AI techniques used for fraud detection include:

Data mining to classify, cluster, and segment the data and automatically find associations and rules in the data that may signify interesting patterns, including those related to fraud.

Expert systems to encode expertise for detecting fraud in the form of rules.

Pattern recognition to detect approximate classes, clusters, or patterns of suspicious behavior either automatically (unsupervised) or to match given inputs.

Machine learning techniques to automatically identify characteristics of fraud.

Neural nets to independently generate classification, clustering, generalization, and forecasting that can then be compared against conclusions raised in internal audits or formal financial documents such as 10-Q.

Other techniques such as link analysis, Bayesian networks, decision theory, and sequence matching are also used for fraud detection. A new and novel technique called System properties approach has also been employed where ever rank data is available.

Statistical analysis of research data is the most comprehensive method for determining if data fraud exists. Data fraud as defined by the Office of Research Integrity (ORI) includes fabrication, falsification and plagiarism.

Machine learning and data mining

Early data analysis techniques were oriented toward extracting quantitative and statistical data characteristics. These techniques facilitate useful data interpretations and can help to get better insights into the processes behind the data. Although the traditional data analysis techniques can indirectly lead us to knowledge, it is still created by human analysts.

To go beyond, a data analysis system has to be equipped with a substantial amount of background knowledge, and be able to perform reasoning tasks involving that knowledge and the data provided. In effort to meet this goal, researchers have turned to ideas from the machine learning field. This is a natural source of ideas, since the machine learning task can be described as turning background knowledge and examples (input) into knowledge (output).

If data mining results in discovering meaningful patterns, data turns into information. Information or patterns that are novel, valid and potentially useful are not merely information, but knowledge. One speaks of discovering knowledge, before hidden in the huge amount of data, but now revealed.

The machine learning and artificial intelligence solutions may be classified into two categories: 'supervised' and 'unsupervised' learning. These methods seek for accounts, customers, suppliers, etc. that behave 'unusually' in order to output suspicion scores, rules or visual anomalies, depending on the method.

Whether supervised or unsupervised methods are used, note that the output gives us only an indication of fraud likelihood. No stand alone statistical analysis can assure that a particular object is a fraudulent one, but they can identify them with very high degrees of accuracy. As a result, effective collaboration between machine learning model and human analysts is vital to the success of fraud detection applications.

Supervised learning

In supervised learning, a random sub-sample of all records is taken and manually classified as either 'fraudulent' or 'non-fraudulent' (task can be decomposed on more classes to meet algorithm requirements). Relatively rare events such as fraud may need to be over sampled to get a big enough sample size. These manually classified records are then used to train a supervised machine learning algorithm. After building a model using this training data, the algorithm should be able to classify new records as either fraudulent or non-fraudulent.

Supervised neural networks, fuzzy neural nets, and combinations of neural nets and rules, have been extensively explored and used for detecting fraud in mobile phone networks and financial statement fraud.

Bayesian learning neural network is implemented for credit card fraud detection, telecommunications fraud, auto claim fraud detection, and medical insurance fraud.

Hybrid knowledge/statistical-based systems, where expert knowledge is integrated with statistical power, use a series of data mining techniques for the purpose of detecting cellular clone fraud. Specifically, a rule-learning program to uncover indicators of fraudulent behaviour from a large database of customer transactions is implemented.

Cahill et al. (2000) design a fraud signature, based on data of fraudulent calls, to detect telecommunications fraud. For scoring a call for fraud its probability under the account signature is compared to its probability under a fraud signature. The fraud signature is updated sequentially, enabling event-driven fraud detection.

Link analysis comprehends a different approach. It relates known fraudsters to other individuals, using record linkage and social network methods.

This type of detection is only able to detect frauds similar to those which have occurred previously and been classified by a human. To detect a novel type of fraud may require the use of an unsupervised machine learning algorithm.

Unsupervised learning

In contrast, unsupervised methods don't make use of labelled records.

Some important studies with unsupervised learning with respect to fraud detection should be mentioned. For example, Bolton and Hand use Peer Group Analysis and Break Point Analysis applied on spending behaviour in credit card accounts. Peer Group Analysis detects individual objects that begin to behave in a way different from objects to which they had previously been similar. Another tool Bolton and Hand develop for behavioural fraud detection is Break Point Analysis. Unlike Peer Group Analysis, Break Point Analysis operates on the account level. A break point is an observation where anomalous

behaviour for a particular account is detected. Both the tools are applied on spending behaviour in credit card accounts. A combination of unsupervised and supervised methods for credit card fraud detection is in.

The following applications of data mining can handle different classes of problems.

Classification: Classification is the most commonly applied data mining technique, which employs a set of pre-classified examples to develop a model that can classify the population of records at large. The literature research says, that classification or prediction is the process of identifying a set of common features, and suggesting differentiating models that describe and distinguish data classes and concepts based on an example. The following example is very nice to understand ‚Classification" in easy words:

A loan creditor must analyze the data to determine which applicants are safe and which can be classified as risky.

The most common data mining techniques for fraud detection are Neural Networks (NN), Naive Bayes, decision tress (DT) and also support vector machines (SVM).

Clustering: In Clustering, as known as cluster analysis the groups of objects, which have a similarity, are identified. The reason to choose the clustering procedure is, that some applications the class affiliation is not available or costly to identify. So the task of Clustering is thus to assign the properties of a feature unclassified record a certain number of clusters. Objects, which are not assigned here, can be assigned in the Data Mining class "outlier detection".

The goal of the cluster analysis is: "Classifying without knowing the classes prior".

The most common clustering techniques are neural networks, Naïve Bayes technique and K-nearest neighbor.

Regression: The goal if regression analysis is similar to the classification technique above. The difference is only that in regression no classes are formed. According to DMG this function is used to determine the relationship between the dependent variable and one or more independent variable.

From the data of a production facility has been recognized, that a certain product parameters correlated very strongly with product quality; now is to find out how these parameters must be set to achieve a specific level of quality .

Common Tools for Regression are linear regression and logistic regression.

Prediction: Prediction is similar to classification. The difference is, that in prediction the exception applies, the results lie in the future. For example, one possible question of prediction analysis would be: "How would be develop the dollar exchange rate in the future".

Neural networks and logistic model prediction are the most commonly used technique in prediction analysis.

Visualization: Visualization refers to presentation of data mining results so that the users can view complex view in the data as visual objects in dimensions and colors [10]. So it is easier for the users to understand the complicated data in clear patterns and use it. "Visualization helps business and data analysts to quickly and intuitively discover interesting patterns and effectively communicate these insights to other business and data analysts, as well as, decision makers." Following visualization and presentation techniques provides this type of data mining technique: trees, tables, graphs, charts, matrices, crosstabs, curves or rules.

Outlier Detection: The aim of outlier detection is to identify data that are not compatible with rest of the dataset. It is one of the most fundamental issues in data mining. A commonly used technique for outlier detection is the discounting learning algorithm.

FRAUD DETECTION AND MANAGEMENT

We can detect various types of fraud using data mining techniques, it may be financial fraud, telecommunications fraud or any computer intrusions. In general, data mining techniques can be classified into two categories according to the type of the machine learning techniques for fraudulent activities it can be detected with the help of supervised and unsupervised learning. Supervised learning for fraud detection involves classification of available record in fraudulent and non-fraudulent categories. Then machines are trained to identify records according to these categories. However, these methods are only capable of identifying frauds that has already accorded.Unsupervised Learning for Fraud Detection method only identifies the likelihood of some records to be more fraudulent than others without statistical analysis assurance. It helps in identifying privacy and security issues in data without using statistical analysis.

CHAPTER – V

CONCLUSION

Researcher has overlooked different data mining techniques for cyber security in banking system. It is a young interdisciplinary field, drawing from areas such as database systems, data warehousing, statistics, machine learning, data visualization, information retrieval, and high-performance computing.

Data mining has great potential as a malware detection tool. It allows you to analyze huge sets of information and extract new knowledge from it. When determining the effectiveness of the methods, there is not only one criterion but several that need to be taken into account. Depending on a particular IDS some might be more important than others. Another crucial aspect Data mining for cyber intrusion detection is the importance of the data sets for training and testing the systems.

The main benefit of using data mining techniques for detecting malicious software is the ability to identify both known and zero-day attacks. However, since a previously unknown but legitimate activity may also be marked as potentially fraudulent, there‟s the possibility for a high rate of false positives.

Future Scope of the project

Banking information systems contains huge volumes of data both operational and historical. Data mining can assist critical decision making processes in a bank. Banks who apply data mining techniques in their decision making hugely benefit and hold an edge over others who don‟t. Some of these decisions are in the areas of marketing, risk management and default detection, fraud detection, customer relationship management and money laundering detection.

Risk Management and Default Detection Every lending decision a bank takes involve a certain amount of risk. Quantifying this risk can make the risk management process easier and limit the risk of financial loss to the bank. Knowing customers‟ capability to repay can greatly enhance a credit manager‟s decisions. Data mining can also help to identify which customer is going to delay or default a loan repayment. This advanced knowledge can help the bank to take corrective measures to prevent losses. For such forecasting, parameters to consider are turnover trends, balance sheet figures, limit utilization, behavioral patterns and cheque return patterns. Historical default patterns can also help in predicting future defaults when same patterns are discovered. Data mining techniques are applied to enhance the accuracy of credit scores and predict default obabilities. Credit score is a value representing a borrower‟s creditworthiness. Behavioral scores are obtained from probability models of customer behavior to forecast their future behaviors in various situations. Data mining can derive this score using the past behaviors of the borrower related to debt repayments by analyzing available credit history.

Marketing is one of the mostly used application area for Data Mining by the industry in general. Banking is not an exception. Retaining customers and finding new customers are getting increasingly difficult because of cut throat competition prevailing in the market these days. Only way to retain a customer or win a new customer is to be proactive and know beforehand what the customer expects and offer him what he wants. This is where data mining can help a great deal. Data mining applied to customer relationship management systems can analyze customer data and can discover key indicators to help the bank to be equipped with the knowledge of factors that affected customer‟s demands in the past and their needs in the future. This enables the bank to targeted marketing. Sequential patterns can be analyzed to investigate changing customer preferences and can approach customers pro-actively. Data mining techniques can help in classifying customers according to the customer‟s

attributes, behavior, needs, preferences, value and other factors. Mainly two scoring models are used for this classification purposes, namely credit scoring model and behavioral scoring model. This classification is valuable information for making customer oriented marketing strategies tailor made for the target category and provide different services for each customer category. For example it can determine how customers will react to a change in interest rates, which customers will be likely to accept new product offers, what collateral would require from a specific customer segment for reducing loan losses. Different levels of analysis like RFM(Recency, Frequency and Monitory) analysis, LTV (Life Time Value) of customers coupled with K-Means clustering can be employed to develop an effective customer segmentation thereby increasing targeted marketing. Data mining can also reveal possibility of cross selling such as selling home loans to credit card customers by analyzing associations from the past data. It can also develop a model of existing home loan customers to analyze their profiles to explore similar customers in other portfolios (like demand deposits or customers with insurance products) to find out potential customers for home loans.

Fraud Detection Banks lose millions of dollars annually to various frauds. Detecting fraudulent transactions can help the banks to act early and limit the damages. Fraud detection is the process of identifying fraudulent transactions from genuine transactions or in other words this process segregates a list of transactions into two classes namely fraudulent and legitimate. Most important area where fraud detection can help is the credit card products. Clustering methods can be used to classify transactions and outliers can be analyzed for frauds. Probability density of credit card user‟s past behavior can be modeled and the probability of current behavior can be calculated to detect frauds. Patterns of customer‟s transactions can be discovered and alerts can be generated if any measurable deviations are found. Financial statement fraud detection is another area that can employ data mining principles to effective use. Banks make credit decisions based on

financial statements produced by customers. These statements may contain overstated assets, sales and profits or it may understate losses and liabilities. Even though these statements may have been audited, these kinds of frauds are hard to detect using normal auditing procedures. Classification techniques based on neural network, regression and decision tree are used for classifying fraudulent ratios in the statements from the non-fraudulent data.

Money Laundering Detection Money Laundering is the process of hiding the illegal origin of "black" money so as to legitimize it. Banks are commonly used as channels to launder money. Therefore governments and financial regulators require banks to implement processes, systems and procedures to detect and prevent money laundering transactions. Failure to detect and prevent such illegal transactions can invite hefty fines both monetarily and operationally which can prove very costly for the bank and even can make its survival difficult. Conventional rule-based transaction analysis based on reports and tools will not be sufficient to detect more complicated transaction patterns like smurfing and networked transactions. Here data mining techniques can be applied to dig out transaction patterns that can lead to money laundering. Typically such systems take client risk assessment data, transaction risk measurement data and patterns and behavior patterns into consideration for detecting money laundering patterns. Transactions are then grouped into clusters based on their similarities found in these chosen attributes. In a large database of banking transactions, it is possible that a huge number of patterns emerge and will be classified as money laundering transactions thereby increasing false positives. Statistical false reduction methods based on decision tree classification are employed to limit the number of false patterns detected.

Investment Banking Investment is an action of investing money into an asset or item for profit/income. Banks often offer investment services to their customers. There are a vast number of financial instruments in the market.

Data mining like K-means clustering can be applied to choose the best investments based on customer‟s profile. Capability to predict asset prices (for example stock prices) from historic prices can increase returns from investment tremendously. Data mining techniques for prediction like neural networks and linear regression can be employed for prediction of prices for stocks. Data mining can also be applied in time series analysis for financial applications.

References

- Bhattacharya.S ,Jha.S, Tharakunnel.K and Westland.C.J, "Data mining for credit card fraud", Science Direct, Decision Support System pp 602-613, 2010.
- Cao.L, Zhang.H, Zhao.Y, Luo.D and Zhang.C,
- "Combined Mining: Discovering Informative Knowledge in complex data", IEEE Transactions Vol. 41 No.3 pp 699-712, 2011.
- Chuang.K.T, Lin.K.P and Chen.M.S, "Quality AwareSampling and its application in Incremental DataMining", IEEE Transactions on Knowledge and Data Engineering Vol. 19 No.4, pp 468-484, 2007.
- Cao.L, "Social Security and Social Welfare Data Mining: An Overview", IEEE Transactions on Systems, Man andCybernetics-Part C: Applications & Reviews Vol. 42 No.6, pp 837-853, 2016.
- Chang.W.H and Chang.J.S, "An early fraud detection methods for online auctions", Science Direct Electronic Commerce Research and Applications, pp 346-360, 2016.
- Clifton.P, Kate.S.M, Lee.S.C.V and Gaylor.R , " Resilient Identity Crime Detection", IEEE TransactionsVolume 24 No.3, March 2016.
- Dharwa.J.N and Patel.A.R, "A Data Mining With Hybrid Approach Based Transaction Risk Score Generation Method for Fraud Detection of Online Transaction", International Journal of Computer Applications Volume 16 No.1, pp 18-25, 2015.
- Drezewski.R, Spielak.J and Filipowski.W, "System Supporting Money Laundering Detection", ScienceDirect Digital Investigations, pp 8-21, 2016.
- Duman.E. and Ozcelik.H.M , "Detecting credit card fraud by genetic algorithm and scatter search", Science Direct, Expert System with Applications 38 , pp 13057-13063,2015.
- Edge.E.M and Sampaio.F.P.R, "The design of FFML: A rule-based policy modeling language for proactive fraud management in financial data streams", Science Direct,Expert System with applications 39, pp 9966-9985, 2016.

- Farvaresh.H and Sepehri.M.M, “A data mining framework for detecting subscription fraud in telecommunication”, Science Direct, Engineering Applications of Artificial Intelligence 24, pp 182-194, 2015.