Available online at https://journalsacfa.apeejay.edu/

ENVISION – International Journal of Commerce and Management
ISSN: 0973-5976 (Print), 2456-4575 (Online)
VOL-16, 2022

Online Banking Frauds and Necessary Preventive Measures

* Dr. Kamal Nain Sharma, **Ankit Kala

ABSTRACT

Banking Industry has undergone digital disruptions at a massive level. Online banking, mobile apps and E-bill payments have become a norm. Banking tractions are digitized from back end to front end and digital transactions are made without any human intervention. The best part is that it is speedy but is it reliable every time? Due to some ignorance or silly mistakes online transactions easily fall into the trap of cyber criminals. This study has been undertaken to analyze online banking frauds such as phishing, smishing, card fraud, etc., and also the causes behind it. The bank staff has been interviewed to understand their perspective on these frauds and whether they have a role to play in such fraudulent activities? Lastly, an attempt has been made to construct a model of the fraud detector system and consequently the preventive methods that can help an individual to stay safe from online frauds.

Keywords: Banking Frauds, Scams, Finance, Behavior, Detection of Frauds

1. Introduction

With the ever-increasing demand of people and thus increasing advancements in technological sectors, we see many illegal activities happening around us. One such activity that has been referred to quite a few times is Online Bank Frauds, often spoken as E-banking frauds. There is a long list of illicit acts that occur under the name of these frauds and in our paper we will be giving an insight about what are the major causes of these frauds and what could be the subsequent cure or prevention measures for keeping ourselves safe from such illegal intentional acts. It is indeed a fact that eradicating banking fraud is a tedious job, but as always prevention is better than cure. (Ram, T., & Acharya, K., 2021).

1.1 Definition

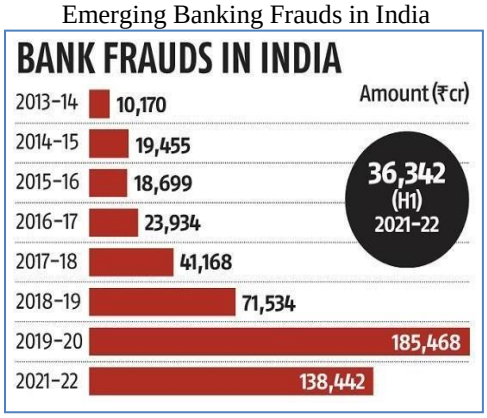
Banking fraud is a term used for acquiring money or any financial possession from financial enterprises such as Commercial Banks, Investment Banks, Insurance companies, etc. by unlawful means. The person who carries out illegitimate deceit is referred to as a scammer, swindler, perpetrator, fraudster, and many more. This law-breaking activity not only hampers the economy of the institution but the nation as a whole.

Many skillful researchers believe that the causes, as well as checks of a financial misdemeanor, are contra-position of the same coin. While in several instances it is considered an offence yet

* Associate Dean Research, LKCTC, Jalandhar, Punjab, India, kamalnain3@gmail.com
**Masters in Computer Applications, Lyallpur Khalsa College Technical Campus, Jalandhar, Punjab, India, ankitkala36@gmail.com

sometimes it might be referred to as a white-collar crime that implies activities or schemes enabling bank theft. (Ram, T., & Acharya, K., 2021).

Figure 1
Emerging Banking Frauds in India



Source: -- business-standard.com

1.2 The known types of banking fraud

Though there are many different types of financial fraud, we will go ahead with the most prominent and well-known ones in our study. In our research, we will examine the artifices first from the customer's point of view and then from the institution's point of view.

Figure 2
Types of banking frauds

(Source: - facebook/oliveboard.com)

1.2.1 Phishing and Spear Phishing

This is the first and foremost attack that compromises the banking credentials of a customer. Phishing is usually attempted through a small email seeking confidential data, but most of these are avoidable these days due to repetitive awareness messages from banks themselves.

Spear phishing is also a targeted version of phishing attacks and they are commonly sent by a trusted source for instance a close relative. It is still advised not to open any link associated with such emails to secure oneself from Trojans and malware.

1.2.2 Spoofing and Vishing

Website spoofing has become an easy job as every other person is learning to code, not necessarily for scamming others but there are certain occasions where people are lured by a clone website of big companies say Amazon, and prompt you to enter your bank details to receive your freebie.

Vishing is again targeted towards confidential details such as user id, login, OTP, CVV, and card pin over a call claiming to be from the customer's associated bank.

1.2.3 Skimming and Smishing

Skimming involves stealing information through the magnetic strip present on the ATM card. The skimmer first scans the credit/debit card and stores its information, sometimes tiny cameras are also used in public locations such as shops, and restaurants to capturecard pins.

Smishing on the other hand is a combination of SMS and phishing, again to obtain personal information. It is advised not to open any link sent in the message box through a toll-free number to avoid this type of fraud.

1.2.4 SIM Swap

Under this scheme, the scammer first issues a new sim card on the customer's current registered mobile number thus receiving all the alerts and OTPs that he requires to easily perform any banking transaction from the customer's bank account.

1.2.5 Credit card fraud

Credit card fraud is a combined term used for all types of scams perpetrated with the help of debit and credit cards. The main reason behind doing so is to obtain services or to pay bills to another account associated with a criminal (Wei, et al., 2013). Around €1.6 billion have been remotely vanished because of this particular fraud last year. 127 million people from the USA have accepted being the victim of credit card theft.

1.2.6 Computer Intrusion

This type of attack occurs when the attackers try to access the entire computer system or a major part of it often referred to as hackers. These intruders used automated computer programs for breaching the computer security (Wei, et al., 2013).

Hence it is advised to ensure a safe system by deploying good antivirus software. Also, data mining techniques now-a-days are very helpful in the detection of computer intrusion attacks.

1.2.7 Telecommunication fraud

Telephony is the oldest massive network encompassing 48% share and hence attackers exploit it very well to gain its benefits. Telecom fraud includes activities directedto gain an advantage over telecom companies.

Many deceptive practices and frauds have been evident so far namely "IRSF fraud" abusing phone rates and "Interconnect Bypass fraud" abusing operator call rates.

1.3 Causes of Banking Fraud

It is not necessary to state that there is no single person responsible for the attack or fraud committed on a financial institution other than the fraudster. There are many substantial reasons, which contribute to the entire process. We are stating all the reviews that we have come across while surveying people at the bank and even the staff at the bank premises. The prominent causes are mentioned hereunder:

1.3.1 Poor internal control

Several times it has been observed that the scams are a due result of the lack of diligence of the banking staff for disbursing loans, more problematic is that this occurs both before and after the disbursal. This clearly shows that low levels of checking and balancing may in turn cause the banking system to fall under the umbrella of fraud.

1.3.2 Poor knowledge of advanced computing

This can also be called technological backwardness in the financial firms, when maximum dependence is given to the manual work instead of using advanced computing resources, it becomes impossible for the untrained staff to supervise huge volumes of banking transactions, increasing the thefts and lowering the fraud detection rate. Hence, it is of utmost importance for financial institutions to train the staff well and equip secure computing resources for controlling the transactions (Khanna, A., & Arora, B., 2009).

1.3.3 Lack of adequate monitoring by the managers

As the subordinates must work well, the same applies to the senior staff i.e. managers of the bank, it is essential to emphasize fraud monitoring systems. These days there are systems available to monitor the credit flow too, but this again creates risks including market risks and operational risks which in turn leads to breaches. Hence it is necessary for the head of the branch to strictly adhere to the process and help the internal auditing team in the detection of any fraudulent behavior.

1.3.4 Unethical behavior at the workplace

Every workplace or firm has become stressful and competitive over time, this includes the financial firms too. Employees feel demotivated due to underpaying, lack of appreciation and often negative reinforcement which leads to unethical practices down the line. Some other reasons could be nepotism in the internal committee causing a breakdown of the moral fiber of Indian banks.

1.3.5 Embezzlement Schemes

If we categorize individuals working in a firm, there is a class of employees that are "opportunist" type. It is often seen that this class of employees perceive the internal problems of the firm very well and then use this slippage to their advantage causing embezzlement or money laundering.

2. Literature Review

The trend of internet usage has touched its peak because smartphones have truly provided customers with digital delights of sharing, transferring, shopping, and receiving funds without

any physical visit to the bank. However, as a bane customers are in deep concern about their privacy and security due to alarming cybercrimes, particularly bank frauds. According to a survey conducted by cybercrime cells, around 1.5 trillion dollars are intruded every year worldwide. Interestingly 60% of these crimes are cropped through smartphones. Studies indicate that there is an immediate need for the detection of these threats. Thus, usage of cybercrime avoidance and prevention tools is very vital for abating e-bank frauds. One more surprising fact that arises from the studies is the excessive use of Trojans (16.98%) and malware (14.55%) accompanied by social engineering practices for conducting bank frauds (Ahmad, I. et al., 2021).

Even though advanced security systems are applied but there are several cases in which they have failed drastically. Hence security systems must be backed up with a fraud detection system for identification of any unauthorized activity but the major problem behind the application of the detection system is that they must be continuously active 24/7. (Kovach, S., 2011).

Some common characteristics of fraud have been noted down by empirical analysts. It includes multiple accounts being accessed by a unique person i.e. fraudster; Small value transactions occur frequently; Payment transactions exceed the daily transaction limit of a customer and repetitive use of forgotten password before large money transaction. These sophisticated traits are widely discussed. Skeptical customers are most active in controlling banking fraud activities. With time advanced data mining algorithms can detect diverse behavior patterns along with imbalanced transactions. This has made it comparably tougher for fraudsters to penetrate the system for a longer time (Wei, W., et al., 2013).

The Trojans are majorly responsible for the attacks; we now clearly visualize how algorithms can detect a Trojan from a genuine customer by using the time stamping mechanisms.

Table 1
Fraudster accessing the portal

Time Page	**Link**
21:55:42.190	Login.aspx
21:55:43.260	BalanceCheck.aspx
21:55:43.890	PayForm.aspx
21:55:44.121	PayConfirm.aspx
21:55:45.091	HomePage.aspx

(Source: Wei, W., et al., 2013)

Table 2
Genuine customer accessing the portal

Time Page	**Link**
21:58:06.190	Login.aspx
21.58.07.391	HomePage.aspx
21:58:15.260	BalanceCheck.aspx
21:58:27.890	PayForm.aspx
21:59:22.121	PayConfirm.aspx
21:59:27.091	Print.aspx
21:59:32.091	HomePage.aspx

(Source: Wei, W., et al., 2013)

The biggest difference that we come across is that Trojan transactions are way too speedyas compared to genuine transactions and homepage of the portal is not visited to save time (Wei, W., et al., 2013).

Many differential analysis algorithms detect these mentioned attributes in a deployed fraud detector system. Even the Reserve Bank of India (RBI) has issued critical guidelines to all financial firms that are prescribed to be followed with strict adherence.

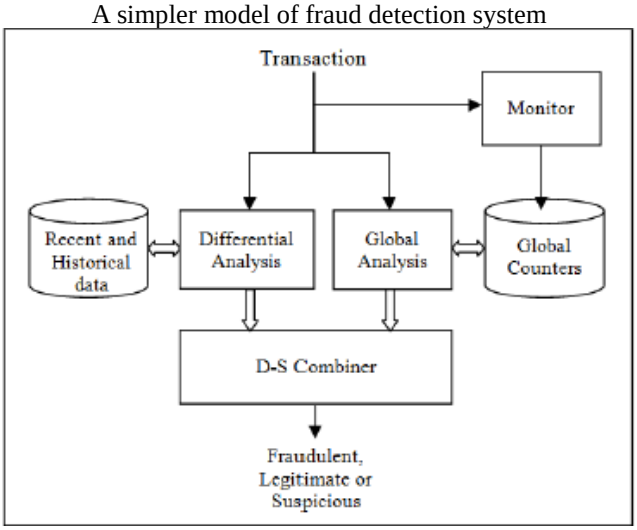
Other six security controls are; internal control, card management, deposits received, passbooks, advances and loans, and handling internal and inter-branch accounts (Khanna, A., & Arora, B, 2009).

Since now, we have come across all the perpetrator cases, it is equally important to gather some evidence that weakens the internal control system of banks to exploit e-banking. This includes personnel threats where bank officials themselves collaborate with the fraudsters to gain benefits.

3. Preventive Methodology

To prevent frauds in banking transactions, two major things are to be considered. Firstly, ensure tight security practices and use of IT especially data mining shall be emphasized for detecting frauds. Secondly, training of bank employees shall be the top priority so as to detect and prevent the frauds at the early stage. A brief design and layout has been given about a fraud detector system below:

Figure 3
A simpler model of fraud detection system



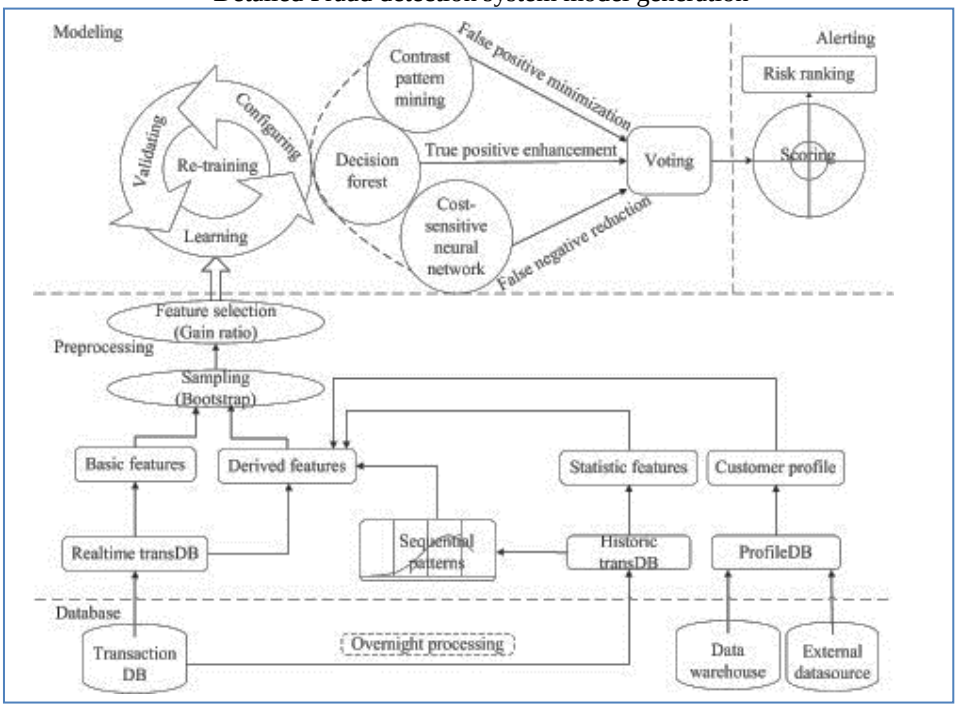
(Source: Kou, Y., et al., 2004)

The above model is a simple architecture proposed by differential analysts. Every device performing banking transactions is subjected to a unique identity and a set of counters is used to measure the transactions. A series of patterns are obtained that predict the unusual behavior from any identified account and whenever unauthorized activity is notched an alarm is triggered (Kovach, S., 2011).

Another important detection system that we came across in our study is more complex as compared to the previous one. This model implies a cost-sensitive neural network for the classification of genuine traits and fraudulent characteristics. Also, decision forests (a combination of varied decision trees) are done in a cascading manner for accomplishing the goal (Alotibi, E. M., 2019)

Figure 4

Detailed Fraud detection system model generation



(Source: Wei. W., et al., 2013)

Data is found and connected via the database tier. Online banking fraud detection information comes from various sources, including real-time transaction logs, recent and historical transaction data, consumer demographic data, and other external sources. Data types and formats vary by source. The pre-processing tier collects real-time transactions, maintains historical data and prepares information for model training and prediction. It also selects and derives essential traits. For real-time fraud detection, too many features reduce model efficiency. This model calculates the significance of a characteristic to each class based on its information gain ratio between the two types and selects those with greater ratios.

Model generation, parameter setting, task scheduling, and retraining are done in the modelling tier. System data mining uses three methods: Using a cost-sensitive neural network to emphasize the higher cost of misclassifying a con compared to a real transaction and a decision forest, which weights individual decision trees by cascading and sharing, to create decision tree ensembles, we find that banking activity is strongly associated with online banking fraud.

4. Conclusion

Security, as well as privacy issues, could be dealt with to a greater extent by the use of global counters, global analysis, and differential analysis. The likelihood of fraudsters accessing the

portal could also be detected beforehand and the overall threat could be minimized. Dempster's rule initiated with the above inputs will yield a suspicion score of every fraud transaction and will be used for future transactions as well.

Other mechanisms can be adapted along with data mining principles namely pattern mining, neural networks, and decision forest. This proves that if IT brings to us cybercrimes, it also brings us the prevention tactics for securing ourselves from such crimes. Finally, technology administration risks tend to decrease with organizational flexibility, staff training and awareness, and support from the top officials to provide a transparent, satisfying working environment based on legal and ethical values. These are perceived inputs for reducing collision among employees so as to reduce banking frauds.

References:

- Ahmad, I., Iqbal, S., Jamil, S., & Kamran, M. (2021). A Systematic Literature Review of E-Banking Frauds : Current Scenario and Security Techniques. *Linguistica Antverpiensia · June 2021*, 3509–3517.
- Alotibi, E. M. (2019). Accounting Management and Its Impact on Detecting and Preventing Fraud in Saudi Banking Systems. *Multi-Knowledge Electronic Comprehensive Journal for Education and Science Publications*, *27*, 1–16.
- Jain, A. & Sarupria, A. (2019). *E- Banking Problems Related to Security and, Privacy Issues along with the traits of Fraud*. 10.13140/RG.2.2.22814.18244.
- Johnson, M. (2008). *A new approach to Internet banking* (Issue 731).
- Khanna, A., & Arora, B. (2009). A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry. *International Journal of Business Science and Applied Management*, *4*(3), 1–21.
- Kou, Y., Lu, C. T., Sirwongwattana, S., & Huang, Y. P. (2004). Survey of fraud detection techniques. *Conference Proceeding - IEEE International Conference on Networking, Sensing and Control*, *2*, 749–754.
- Kovach, S. (2011). Online Banking Fraud Detection Based on Local and Global Behavior. *ICDS 2011 : The Fifth International Conference on Digital Society*, *January*, 166–171.
- Ram, T., & Acharya, K. (2021). Banking Frauds : Causes and Preventions. *Journal of Banking, Finance & Insurance*, *2*, 70–77.
- Wei, W., Li, J., Cao, L., Ou, Y., & Chen, J. (2013). Effective detection of sophisticated online banking fraud on extremely imbalanced data. *World Wide Web (2013)*, *16*, 449–475.