Int. j. adv. multidisc. res. stud. 2023; 3(3):1124-1127

Received: 07-05-2023
Accepted: 17-06-2023

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Significant Role of Digital Technology in Detecting Banking Frauds in India

[1] Dr. Chittimalla Bhargavi, [2] Dr. Sravanthi M

[1] Assistant Professor, Vaagdevi College of Engineering Autonomous, Warangal, Telangana, India
[2] Assistant Professor, Vaagdevi College of Engineering (MCA), Warangal, Telangana, India

Corresponding Author: **Dr. Sravanthi M**

Abstract
The transition of banking to digital channels is causing a revolution in financial fraud. Fraud is a major issue for banks and financial institutions. Every year, billions of dollars are wasted to fraudsters who find methods to exploit system flaws. That is why it is critical to have strong fraud detection procedures in place. Fraud is a significant issue that has an impact on individuals, businesses, and banks alike. Fortunately, there are some digital technology that may be used to detect and stop banking fraud and scams. This research paper highlights that Banks and businesses can help safeguard themselves and their clients from fraudsters by utilizing technologies like machine learning algorithms, Artificial Intelligence, multi factor authentication, and fraud detection software. Artificial intelligence technology is particularly effective in detecting scams, with 63 percent of financial institutions stating that AI is capable of preventing cyber crime before it occurs.

Keywords: Transition, Frauds, Fraudsters, Banks, Digital Technology, Detection

Introduction
An effort to steal money or assets from a financial institution is referred to as banking fraud. Fraud, according to the RBI, is "any person's deliberate act of omission or commission in the course of a banking transaction or the books of accounts maintained manually or under computer system in banks, resulting in wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank." Bank fraud accounts for a sizable portion of white collar crimes investigated by authorities. Unlike most crimes, the amount stolen in these frauds is in the thousands and crores of rupees. Bank fraud is a federal offense in several countries, defined as attempting to obtain property or money from any federally insured financial institution. According to the RBI's Financial Stability Report, in recent years, the Indian banking industry experienced 2,331 fraud incidences worth Rs. 87 crores. In the previous six months, there has been an increase in bank fraud involving cards, the internet, and currencies.

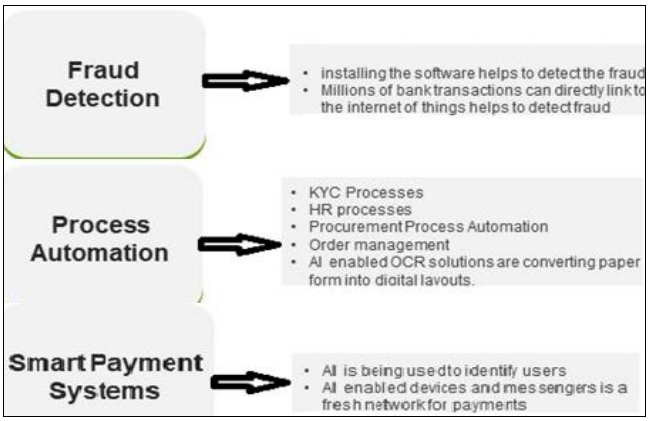
Objectives of the Study
1. To know how digital technology used in detecting banking frauds.
2. To explore the stakeholders how to protect themselves against banking frauds.

Digital Technology Used in Detecting Banking Frauds
During pandemic the world has shifted towards digital payments, which led to frauds become more common than ever. The digital revolution has enabled numerous new types of banking frauds. Fraudsters were benefited with advanced technologies, are continuously looking for new vulnerabilities in committing crimes. With the help of advanced technological tools such as machine learning and AI, not only banks, neobanks and financial institutions are able to detect and prevent the frauds but also credit cardholders can be alerted to respond before fraudsters steal a considerable amount of money from their credit or debit cards.

Fraud Detection System Using AI Technology:
FDS is the process of identifying financial frauds instead of reinforcing security from the point of view of service users; therefore, it is accompanied by increasing the individual security consciousness of the parties involved in the transaction, challenging to detect as the volume of electronic financial transactions and the frequency of the payments have been increased with the diversified payment methods. This will not only strengthen the technological security system but it will also have a direct impact on the decrease of potential phishing damages.

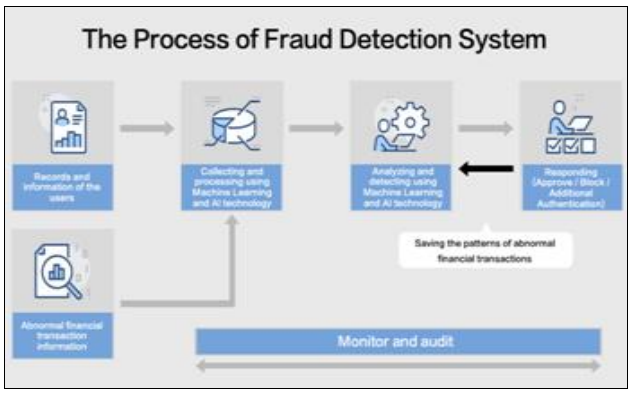
One of the most notable elements of FDS is the use of AI technology is a fast effective and efficient application which prevent frauds and assess the risk in order to achieve greater effects in the information collecting, processing, and detection processes. FDS has been organized and operated as follows:

1. Collecting and Processing the Information: By accumulating as well as processing the information via the user's financial transaction device, the data is employed to the necessary form in the next step by means of quality enhancement and quantitative reduction. In this procedure, machine learning is employed for operational data processing.



2. Analyzing and Detecting: Analyzing the transactions is one of the important financial functions. This step uses machine learning to detect abnormal transactions by examining earlier processed financial transaction data and accumulating abnormal financial transaction patterns. Various AI analysis techniques, such as detecting data misuse, abnormalities, and hybrid detection utilizing deep learning, are applied in this situation.

3. Responding: Additional authentication is performed in this stage for the approval and blocking of abnormal transactions. Furthermore, data collection and notification to the administrator and users may occur.



4. Auditing and Monitoring

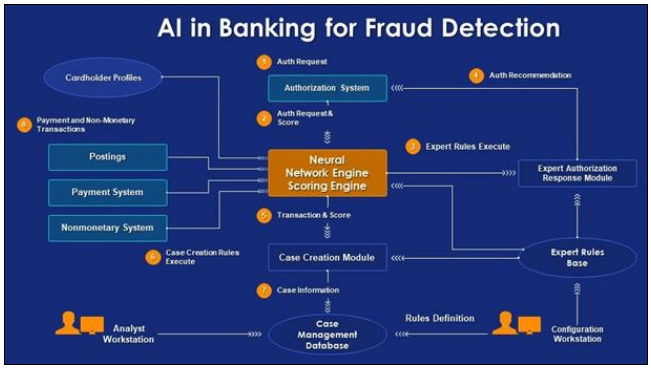
The auditing and the overall monitoring of the Fraud Detection System process in finding the abnormal transactions.

As a result, FDS is more active in detecting and stopping of abnormal transactions than standard security solutions in financial organizations such as banks, credit card firms, or Internet spaces that have payment platforms.

Ways of Fraud Detection in Banking Using AI:

Building Purchase profiles: To detect the fraud, first we need to understand the typical consumer behaviour. With the machine learning application we can sort the vast amounts of data from past financial & non financial transactions, banks are able to build the profiles of their customers which exhibit the up to date picture of the activities of the customers that can help the banks to predict their future behaviour.

Developing Fraud Scores: Using data from previous legitimate transactions, fraud incidences, and risk parameters defined by the financial institution, all transactions can be assigned a fraud score. The score, which considers characteristics such as transaction amount, duration, card use frequency, IP address of a purchase, and other factors, is used to quantify the fraud risk associated with that specific transaction. Fraud ratings are used to approve a transaction automatically, flag it for review, or reject it entirely. Machine learning enhances the accuracy of fraud scores over time.



Fraud Investigation: Machine learning algorithms can examine hundreds of thousands of transactions every second, making them ideal for fraud detection. Neural networks extend this power by making decisions in real time. These technologies are effective in reducing the huge amount of detected transactions and providing a short list of those that require further investigation by a human the same. Investigating and prosecuting fraud allegations may be extremely time-consuming, therefore equipping agents with the necessary tools to boost efficiency is critical. This augmented intelligence tool can assist teams in prioritizing and streamlining investigations.

Know your Customer: Based on artificial intelligence KYC methods can instantly validate ID and paperwork, match fingerprints, and even perform facial recognition. This effective solution finds the ideal mix between client security and convenience. Consumers continue to seek to financial institutions to give mobile banking and internet access to their information. In addition, customers expect their bank to establish a safe and secure environment within which these transactions can be executed. There are certain issues such as:

- **Mail Phishing:** is done by sending fake messages and sites to user's mail id with the intention to retrieve the confidential information and attacks the system and steals the valuable data and money. Hence ML

algorithms can differentiate between the legitimate and spam mails in order to avoid the fraudulent activities.

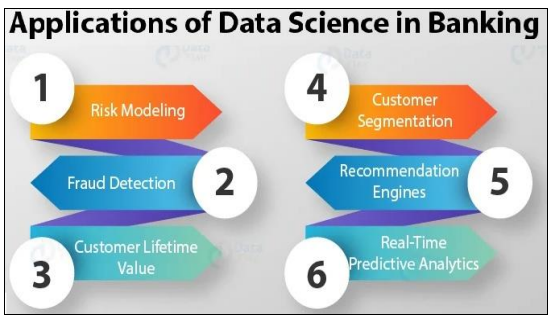
- **Identify Theft:** AI can be used to identify theft by implementing the effective security features like multi factor authentication and human like intelligence. With this facility the users can get the notifications immediately if one changes their passwords or any updates are made to their identity. AI can help the banks in real time and prevents their users from fraudulent activities.
- **Credit Card Theft:** The fraudsters can also access your credit card details by email phishing or identity theft for purchases without physically processing the card. AI solution can quickly detects when buyer behaviour are mimicked and if something goes wrong and notifies immediately and their by the card can be blocked immediately in real time to prevent the fraud.
- **Forgery of Documents:** Machine learning algorithms and AI were trained well enough in detecting the forged ID, and differentiates between the fake and original ID with the increase in the number of datasets, the accuracy rate of detecting such fraudulent activities were increased, and thereby supporting the banking institutions to provide fool proof solutions to their customers.

Big Data Analytics in Detecting Frauds in Banks:

Big Data analytics is a strong and sophisticated tool for not only detecting security issues and fraudulent activities, but also preventing them from occurring in the first place to address global cyber security threats. Banks are also increasingly using data analytics to detect fraud and also for customer retention. Banks can look for patterns that may indicate fraud by examining massive data sets. Analysis the fraud based on end-point centric (the users and their end points), navigation centric (analysis the navigation behaviour and suspects pattern) and account centric (analysis the abnormal behaviour) for example, if a customer suddenly begins making a large number of little transactions that are all just below their daily limit, this could indicate that they are attempting to avoid activating fraud detection mechanisms.

Data Science in Banking:

Data Science in banking industry helps to formulate credit risk modeling strategies to reinforce the lending schemes and classifies the defaulters before sanctioning loan in a high-risk scenario. Fraud detection involves monitoring and analysis of the user activities, customer segmentation, and strengthening relationships with their customers and nurtures them for the current as well as future prospects, real time predictive analysis.



Data Mining to Detect Banking Frauds:

The ability to detect fraudulent behaviors is becoming increasingly important for many firms, and with the help of data mining, more fraudulent actions are being recognized and reported. The bank also uses data mining for fraud detection and protects the customer's funds from credit card frauds. The profiles of the customers can be gathered through data mining to pitch new products and services this helps to retain the existing the customers and targets the new customers. Initially the banks tap the data warehouse of third party (which may contain transaction information from multiple organizations). The bank can then compare those patterns to its own database to look for signals of internal instability. The fraud pattern recognition is only dependent on internal bank data.

Tips for the Stakeholders to Protect Themselves against Banking Frauds

- Shoulder surfing is the practice of spying on someone when they are using an ATM or entering personal information into a phone in order to steal their data. Be cautious of shoulder surfing.
- Take advantage of the ability to set and change your transaction limits on your cards and account. Don't Share any of your personal details about your finances on social media.
- When utilizing a personal laptop for business, create a separate user account and Keep your PINs private
- Don't give someone your account information or fill it out on a website until their identification can be verified. Put your money in a reputable financial institution. Don't hand your money to someone who offers to deposit it in a bank on your behalf in exchange for a better interest rate. Report any unusual activity in your bank account or while using your credit card.
- Examine your monthly credit card statements thoroughly. Take caution when making online payments. Only on secure payment websites should you enter your Card Verification Value (CVV).
- Do not reveal your OTP to anyone. Check that the OTP produced is for the transaction that you initiated.

Conclusions and Suggestions

As the Banks protects the money of public, the employees of the bank must be cautious and diligence while performing the transactions. In the present scenario banking fraud has turned into a significant business. Every year, massive losses are caused by digital fraud in the banking industry. Thus, in modern the AI and big data analytics plays a vital role in the digital transformation are the bank's secret weapon that is helping in identifying and preventing frauds before it happens in banking. Data mining in banking sector mainly useful for retention and targeting the new customers, automatic credit approval for fraud prevention and providing segment-based products and services, fraud detection in real time by analyzing risk. Educate both employees and customers about phishing and social engineering attacks and alert the customers by sending notification whenever there is a suspicious activity. In online banking system the banks must incorporate fraud monitoring system and must manually review the reports daily. Never and ever use the public Wi-Fi and Multi-factor authentication can be used to prevent credential stuffing.

References

1. Swain DS, Pani DL. Frauds in Indian Banking: Aspects, Reasons, Trend-Analysis and Suggestive Measures, International Journal of Business and Management Invention. 2016; 5(7):1-9.
2. Bhasin ML. Fraud Scenario Prevalent in the Banking Sector: Experience of a Developing Country, the East Asian Journal of Business Management. 2016; 4(4):8-20.
3. Gupta PK, Gupta S. Corporate frauds in India-perceptions and emerging issues, Journal of Financial Crime. 2015; 22(1):79-103.
4. Anthala HR. Research paper on Case laws of Fraud, forgery, and Corruption in Banks and Financial Institutions in India, IOSR Journal of Economics and Finance. 2014; 3(6):53-57.
5. Kundu S, Rao N. Reasons for banking fraud-A case of Indian public sector banks. International Journal of Information Systems Management Research & Development. 2014; 4(1):11-24.
6. Rajdeepa, Nandhitha. Fraud Detection in Banking sector using data mining, IJSR. 2015; 4(7):1822-1825.
7. Anil Dogra. Banking Frauds in India: Case studies of Nirav Modi and Vijay Mallya Case, IJCRT. 2018; 6(1):855-860.
8. Madan Lal Bhasin. Combatting Bank Frauds by integration of technology: Experience of a developing country. British Journal of Research. 2016; 3(3):64-92.
9. Kaveri VS. Bank Frauds in India: Emerging challenges, Journal of Commerce and Management thought. 2014; 5(1):14-26.
10. Pan S. An Overview of Indian Banking industry, International Journal of Management and Social Science Research. 2015; 4(5):67-71.