

18

Chapter

FINANCIAL FRAUD AND ITS PREVENTION BY ARTIFICIAL INTELLIGENCE TECHNIQUES

Dr. Neha Singh

*Assistant Professor, Department of Management,
BBD university, Lucknow*

Dr. Zia Afroz*

*Assistant Professor, Department of Humanities and
Social Sciences, Integral University, Lucknow*

**Correspondence to: vint1983@gmail.com*

Dr. Rupali Sharma

*Assistant Professor, Department of Education,
Sri Mahesh Prasad Degree College, Lucknow*

Arbaaz Khan

*Assistant Professor, Glocal School of Business and
Commerce, Glocal University, Saharanpur, U.P.*

Email id: arbaaz@theglobaluniversity.in

DOI: <https://doi.org/10.52458/9789388996969.nsp2023.eb.ch-18>

Ch.Id: [GU/NSP/EB/ESTDCI/2023/Ch-18](#)

ABSTRACT

Financial fraud is very important concern is now a day as the population is involving in online or digital mode of payment methods. The financial fraud reported in 2022 survey reported that around 42% Indians had their experiences in past few years and in many cases around 74% after making complaint they have not returned back their money. The financial frauds are possible with mobile phones, online transaction, money laundering etc. The chapter is an attempt to explore various types of financial frauds and its effects on the individuals as well as organization.

Keywords: *Financial Fraud, Artificial Intelligence Techniques, Money, Banking, Non-Banking, Finance*

17.1 INTRODUCTION

Financial Fraud: When someone digitally steals the money causing an adverse effect on our financial condition through illegal practices is known as financial fraud. Even as digital payments continue to gain prominence in India, with most Indians resorting to Gpay, Phonepe and other apps, the financial fraud encountered has also risen. A survey conducted by private firms Local Circles in 2022, has shown that 42% of Indians surveyed experienced financial fraud in the last 3 years, and 74% of those who experienced it failed to get the money back (Bao et al., 2022).

There are many types of financial fraud, some are explained below: -

1. Mobile fraud
 2. Credit Card fraud
 3. Money Laundering
 4. Identity fraud
 5. Internal fraud
 6. Bank fraud
 7. Phishing
- a. **Mobile Fraud:** An Internet **bot**, web robot, robot or simply **bot** is a software program that operates on the Internet and performs repetitive tasks. In the year 2016, bot was created by a fraudster on Facebook through which about 10,100 accounts were hacked by offering the users to install the browser extensions. User's personal data including financial sites were hacked. Fraudster used to make phone calls to the users and claim that you have won the lottery and asks

your personal details to transfer the money but at the end the money from our account is transferred to fraudsters account

- b. **Credit Card Fraud:** This type of fraud is a common type of digital crime or cybercrime. Credit card fraud is an inclusive term for fraud committed using a payment card, such as a credit card or debit card. The personal data of the users can be hacked by phone calls, wi-fi hotspots and emails to make payment to another account, which are controlled by a criminal for which they do not need to hold your card in their hands.
- c. **Money Laundering:** Money laundering is the illegal process in which a large amount of money is generated by criminal activity like terrorist funding and drug trafficking. The money from the criminal activity is illegal but the launders make it look legal. The origin of the money is illegal, but it looks legal.
- d. **Identity Fraud:** identity piracy or identity infringement occurs when someone uses personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes. Fraudsters commit identity fraud when a user uses internet banking via the internet. They obtain the personal data which is used to steal the money digitally.
- e. **Internal Fraud:** In this, the fraud is committed by an employee against the organization. The employee uses the resources and assets of other employees for their own personal use. As stated by NetGuardians, 70% of banking fraud is internal and most of them remains undetected. This happens because an employee is a trusted person who has little supervision.
- f. **Bank Fraud:** Bank fraud is the use of potentially illegal means to obtain money, assets, or other property owned or held by a financial institution, or to obtain money from depositors by fraudulently posing as a bank or other financial institution.
- g. **Phishing:** It is an attempt generally made by cyber-criminals posing as legitimate institutions, through e-mail, in order to get critical information from the targeted individuals. The practice of deceiving, pressuring or manipulating people into sending information or assets to the wrong people. It is a type of social engineering and scam where attackers deceive individuals into disclosing critical information / installing malware such as ransomware (Choi and Lee, 2018).

17.2 ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI), a groundbreaking concept that once solely belonged to the realm of science fiction, has now become an essential part of our lives. At its core, AI refers to build computer systems which can perform those tasks that needs human intelligence. From natural language processing to machine learning algorithms, AI continues to astound with its capabilities. Few applications include- AI in healthcare, astronomy, gaming, education, data security, social media, detecting financial fraud, etc (Cross, 2022).

AI works on a foundation of special software and hardware for training and writing the machine learning algorithms with the help of programming languages like python, R and java. AI works on combing the large amount of data with intelligent algorithms which allows the software to lean automatically from the patterns which is present in data, there are various subfields of AI included in the Artificial Intelligence Technique which are:

- Deep Learning.
 - Computer Vision
 - Machine Learning
 - Natural Language Processing
 - Robotics
 - Fuzzy Logic
 - Expert System
- a. **Deep Learning:** Deep Learning takes ML to a higher level by employing neural networks with multiple layers to process complex data representations. It has propelled AI achievements, such as beating human champions in games like chess and go and enhancing image and speech recognition systems.
- b. **Computer Vision:** One of the most popular branches of artificial intelligence right now, computer vision, focuses to build techniques that help computers to see and understand digital images & videos. Computer Vision equips machines with the ability to interpret visual information from the world. This technique has revolutionized industries like healthcare, automotive, and robotics, enabling tasks such as facial recognition, object detection, and autonomous driving. Computer vision has applications across industries, such as:

- Object tracking. Following or tracking detected objects.
 - Image classification. An image is classified and accurately predicted to belong to certain classes.
 - Facial recognition. Face unlock on smartphones unlocks devices by mapping and matching facial features.
- c. **Machine Learning:** is the field of artificial intelligence in which machines learn several concepts using data using statistical analysis to predict input data as output value. This field is divided into supervised and unsupervised learning depending upon the learning method. In supervised learning the value of input data is predicted and classified with the given label and in unsupervised learning the data is not labeled and is also called clustering process. Machine learning algorithms are classified into three types:
- **Supervised Learning** - Machines are competent with the labeled data to predict the outcome.
 - **Unsupervised Learning** - Machines are made competent with unlabeled data, with the model extracting information from the input to identify features and patterns, so it can generate an outcome.
 - **Reinforcement Learning** - Machines learn through trial and error, using feedback to form actions and machines more seamless than ever to fraud detection.
- d. **Natural Language Processing (NLP):** It lets machines to comprehend, interpret, and generate human language. This AI technique has paved the way for virtual assistants, chatbots, and language translation tools, making communication between humans (Sood et al. 2023).

Some NLP examples are:

- **Virtual Chatbots** - They can recognize contextual information to offer customers better responses over time.
- **Spam Detection** - NLP text classification can scan language in emails to detect phishing or spam.
- **Sentiment Analysis** - Analyzing language used in social media platforms helps to extract emotions and attitudes about products.

17.3 CONCLUSION

The policy making institutions has developed the protective measures for such financial frauds but still it is not sufficient up to certain level. The platforms like Facebook or others are also being affected due to such financial frauds. Financial frauds by credit card, debit card has reached to the alarming stages in many senses after making protective system by the banking and non-banking financial institutions and is also noted that the personal details by these credit and debit card is under the threat zone. Emerging protective technologies are playing protective measures for preventing such financial frauds.

REFERENCES

1. Bao, Y., Hilary, G., & Ke, B. (2022). *Artificial intelligence and fraud detection. Innovative Technology at the Interface of Finance and Operations: Volume I*, 223-247.
2. Choi, D., & Lee, K. (2018). *An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation. Security and Communication Networks*, 2018.
3. Cross, C. (2022). *Using artificial intelligence (AI) and deepfakes to deceive victims: the need to rethink current romance fraud prevention messaging. Crime Prevention and Community Safety*, 24(1), 30-41.
4. Sood, P., Sharma, C., Nijjer, S., & Sakhuja, S. (2023). *Review the role of artificial intelligence in detecting and preventing financial fraud using natural language processing. International Journal of System Assurance Engineering and Management*, 1-16.