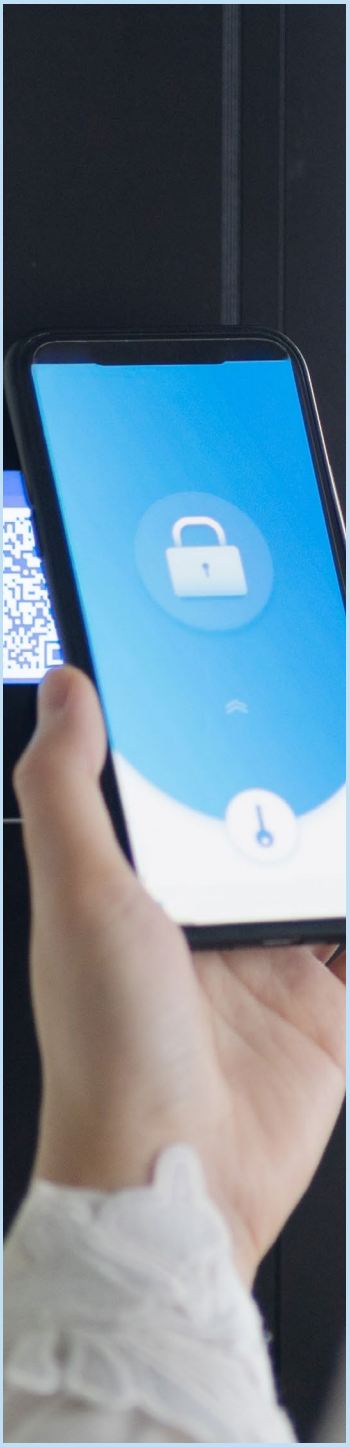
VIEW POINT



FRAUD DETECTION AND PREVENTION – ROLE OF TECHNOLOGY IN FIGHTING FIRE BY FIRE

Abstract

Fraud Management has been a challenge to organizations for decades. Traditional fraud management was primarily manual and time-consuming, leading organizations to invest heavily in manpower and effort, yet still failing to prevent frauds. With each decade, technologies have evolved drastically, especially in the last decade with the emergence of various new technologies like Blockchain, IoT, Metaverse, AI, and more recently, Generative AI. This has also led fraudsters to adopt the same technology, resulting in new fraud types. In this PoV, we explore the genesis of fraud and its evolution. We touch upon the role of technology in assisting fraudsters to commit these frauds and explore various AI/Generative AI technologies that organizations can leverage to tackle the same frauds, essentially fighting fire with fire.

Infosys®
Navigate your next

Table of Contents

Background

Let me begin by telling a small story. Two Greek sea merchants, Hegestratos and Zenosthemis took an insurance policy (known as bottomry in those days) on their cargo and ship. According to the agreement they would repay the loaned money after selling their merchandise along with interest amount. Upon failure of payment the lender would gain possession of both the cargo and ship.

Once they set sail, they decided to sink the ship so that they could claim all the loaned money. As things would turn out they were caught in the act and Hegestratos lost his life attempting to escape, and Zenosthemis faced wrath of the law in Athenian courts. This happened in 300 BC! Fraud has existed for more than 20 centuries now. Fast forward to recent years PwC's 2022 Global Economic Crime and Fraud survey reported a 42 billion US dollars fraud loss!

Evolving Landscape of Managing Frauds

Fraud is considered to have happened when an act is committed by one or more people intentionally where the act is deemed to be illegal, and the end result of the act is to get financial gains or power usually. With changing times and technology, Fraud techniques and patterns have significantly changed and with the advent of Generative AI this is now posing serious challenges globally.

This evolution can be broadly classified into 4 stages:

Evolving Landscape of Managing Fraud

Manual and Reactive	Early fraud detection was done manually by organizations which is purely reactive in nature and laborious to identify suspicious patterns and report the same and was very time consuming
Rule Based Engines	With Changing landscape manual process changed to rule based approach with predefined rules built into systems to detect frauds and highlight the same as an improvement over manual detection
Leveraging AI/ML	Leveraging AI/ML for fraud management catapulted fraud detection into a new era in fraud management With tons of data at disposal, AI/ML helped identify complex fraud patterns real time enabling organizations put preventive actions
MFA and Biometrics	With more sophisticated scams in addition to technology, organizations have introduced additional measures of security by introducing MFAs and Biometrics with the use of technology

Current State of Fraud with Technology Advancement

With Generative AI, technology is changing at a rapid pace and organizations have started adopting this across multiple industry segments. The flipside of it though is, with widely available and free to use Generative AI tools, Fraudsters have also evolved further leveraging the same technology. They are becoming more sophisticated and committing frauds using Deepfakes, Generative AI generated Phishing Emails, Synthetic PII, Generative AI Chat bots etc.

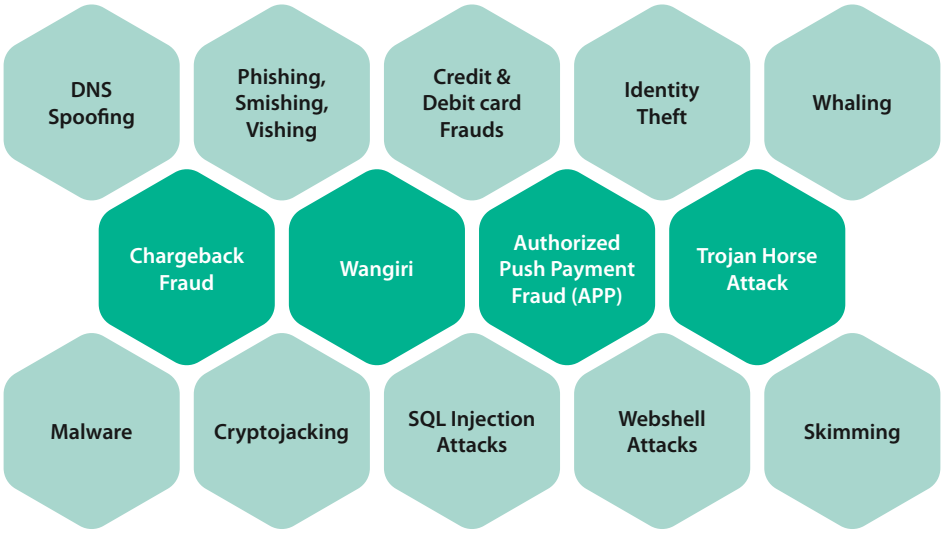
They are also ensuring that the power of Large Language Models (LLMs) is being fully exploited and creating fraudulent content like:

- **FraudGPT** is a subscription-based malicious Generative AI. It leverages sophisticated ML algorithms to create deceptive content, offering a wide range of capabilities for malicious purposes. It can create spear phishing emails, fraudulent invoices, fake news articles, etc., and can be used in cyber-attacks, online scams, public opinion manipulation, and so on.
- **Deepfakes,** for example generate audio, video and or images which is becoming next to impossible to identify the same from genuine content.
- Create **chatbots** or **phishing mails** which help steal vital information from businesses, individuals alike.
- Generating **Synthetic content** to create identities and generate fake PII data through few prompts at scale in addition to creating deepfakes of people who have never existed.
- **Authorized push payment** frauds are perpetrated through deepfakes, Generative AI chatbots, and Generative AI generated phishing emails, which make content appear authentic to customers.

In short Generative AI has opened up many new ways to create content and deceive people and is resulting in distinguishing authentic content from synthetic content next to impossible.

Types of Fraud

Some of the most common types of frauds which people fall for are listed below. These frauds can occur on a wider range of platforms targeting users in mass.



Fraud Management Challenges Faced by Organizations

Technology has changed the way we do business today and with new ways of working, it has also resulted in opening avenues for fraudsters to exploit the shortcomings of new ways of working. Some of the challenges faced by organizations today to counter fraud are:

- Existing methods of fraud prevention have not evolved to the scale which will ensure they can prevent all kinds of frauds.
- The ever-increasing availability of data poses more challenges for training and evolving existing models to counter new fraud types.
- With everything going the digital way it has created multiple channels for fraudsters to commit frauds (Web, mobile, offline etc). As a result, analyzing complex patterns across these channels to derive insights for fraud prevention is more complex than before.
- High false positive rates leads to authentic transactions being flagged as fraudulent causing significant impact to end customers where real fraud detection is missed out.
- Flagging frauds real time and taking immediate preventive action is evolving while organizations grapple to identify new fraud patterns.
- Higher costs to train, maintain and deploy LLMs due to large data volumes.

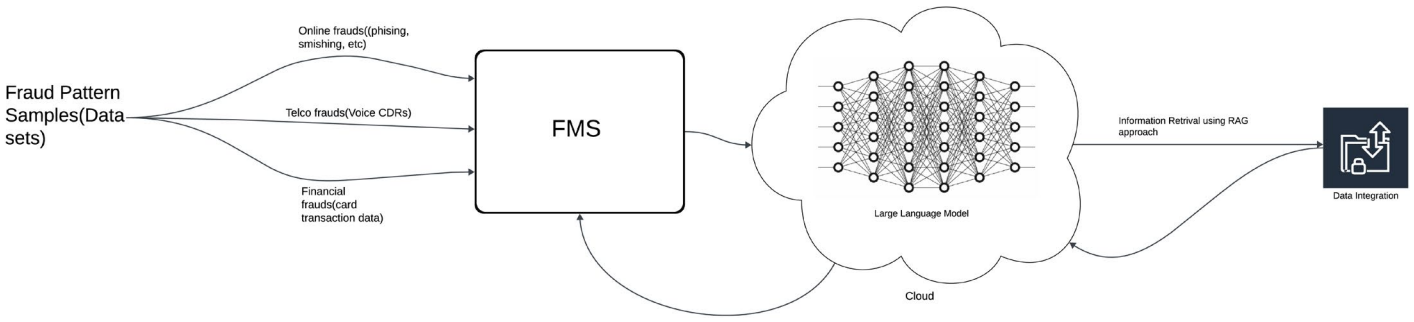
The below table shows types of frauds experienced by merchants - Past 3-year rankings and global incidence.

	2021 Rank	2022 Rank	2023 Rank	Global % Experiencing (2023)
Phishing / pharming / whaling	3	1	1	**43%** ↑
First-Party Misuse (i.e., friendly / chargeback fraud)	1	4	2 ●	34%
Card testing	2	2	3 ●	33%
Identity theft	4	3	4 ●	33%
Coupon / discount / refund abuse	5	7	5 ●	30%
Account takeover	7	5	6 ●	27%
Loyalty fraud	6	6	7 ●	22%
Affiliate fraud	8	8	8	22%
Re-shipping	12	11	9 ●	**20%** ↑
Botnets	10	9	10 ●	19%
Triangulation schemes	9	10	11	17%
Money laundering	11	12	12	15%
AVG. # of attacks experienced	**3**	**3**	**3**	**3**

● Increased Risk ● Decreased Risk ↑ Sig. Higher vs. 2022

Role of Technology in Fighting Frauds

Fraud prevention is more important than fraud detection. Organizations are aiming at preventing occurrences of frauds in the first place as a proactive approach rather than reactively detecting frauds once they have already occurred. Technology has been and will be the backbone of building solutions in every industry/domain and will also play a huge role in fraud prevention. AI techniques like anomaly detection, pattern recognition, Large Language Models (LLMs), Natural Language Processing (NLP), Multimodal learning etc. can be used extensively to detect and prevent frauds. In simple terms, AI models work on the principle as shown in the below diagram.



While Generative AI is being leveraged by fraudsters to exploit it and commit frauds, it has ensured its role in fighting these same frauds. Its ability to identify complex patterns and implement proactive measures helps in minimizing evolving fraudulent activities.

Generative AI can play a huge role in:

Real Time Analysis
Pattern Identification of fraudulent activities Real Time for preventive actions

Pattern Identification
Identifying complex patterns from large data sets to increase accurany and reduce hallucinations

Anamoly Detection
Detecting Anamolies by identifying deviations from baselines

Machine Learning
Evolving and adapting to new fraud techniques through historical data analysis

Big Data Integration
Analysis of large volumes of Data to identify correlations and patterns to improve the accuracy and effectiveness of the models

Some of the advanced technologies which can be leveraged for early detection and prevention of frauds are:

Graph Neural Networks (GNN)

GNNs has the capability to expose suspicious activities by scanning through billions of records and identify unknown patterns of activity and make correlations to detect if an account in past sent transaction to suspicious account(s). GNNs build representation concept within the model of local structure and feature context. Information from node and edge features is propagated along with aggregation and message passing through various neighboring nodes.

When GNNs run several layers of graph convolution, the final node state has data/information from nodes multiple hops away. The GNNs larger receptive field can then track more longer and complex transactions used by financial fraudsters who try to cover their tracks.

The other advantage of GNNs is it can also train on self-supervised or unsupervised tasks.

Retrieval Augmented Generation (RAG)

Retrieval-Augmented Generation (RAG) is a technique designed to enhance the precision and dependability of Generative AI models by incorporating factual data/ information from external repositories. In the case of fraud detection, it provides many benefits by leveraging these data sources to provide Enhanced data integration, improved accuracy, real-time responses, scalability, etc.

Generative Adversarial Networks (GANs)

A Generative Adversarial Network (GAN) is a deep neural network which has the ability to learn from a set of data and then generate new data which will display similar characteristics of the training data set. The fraud patterns are similarly trained to these networks to distinguish between the real and fake ones. It is important to note that the Generator network should not be able to fool the discriminator from the real and fake in which case the purpose gets lost.

Convolutional Neural Networks (CNN)

Convolutional Neural Networks are deep learning neural networks which process structured arrays of data like images and pick up patterns and help in detecting anomalies like facial features displaying emotions, inconsistent facial movement patterns, discrepancies in the shading of facial skin tone, etc. in deepfakes. They effectively pick up on patterns in an image including gradients, facial lines, circles etc. and can work on a raw image without any preprocessing. This will aid organizations to leverage the same to detect deepfakes primarily.

Autoencoders

Autoencoders are neural network-based models used for unsupervised learning and discover correlations among represent data and data in smaller dimensions. The autoencoders frame unsupervised learning problems as supervised learning problems to train network models. The input itself gets passed as output and the input is squeezed to lower encoded representation through encoder network, and then the decoder network decodes the encoding to recreate input. The encoding displays a lower-dimensional representation of data and shows complex relationships among data. This can thus be used to derive complex patterns in frauds enabling to detect fraud early by leveraging large data sets.

Advanced Analytics to Monitor Every Customer Touchpoint

Customer touchpoints are many for organizations and each of these points need to be monitored for rich data insights to prevent frauds. Customer touchpoints range from social media, sales channels, industry events, customer support channels, internal data sources, marketing campaigns to customer surveys reviews, etc. The focus will be more on predictive analytics to mine data for insights to derive fraud patterns and aid in taking preventive actions.

Fraud Trends to Watch Out for in 2024

Some of the frauds trends to watch out for in 2024 will include

- **Advancements in Deepfake Technology** – Impersonating individuals, causing identity theft and posing major threats to customers and organizations including Deepfakes simulating speech, emotions and human actions.
- **Synthetic Identity Theft** – Synthetic identity theft results fake identities with real data like address for example and fabricate information making it highly challenging to identify frauds. Since there are authentic components as well it complicates fraud detection further.
- **Account Takeover Frauds** – Involves gaining unauthorized access to real customer data across their accounts which includes social media, financial accounts etc. and using the same to commit financial frauds, identity thefts etc.
- **Social Engineering Attacks** – this works on human psychology and persuades customers to engage in unsafe activities for example clicking on malicious links which will lead to divulging customer PII.
- **Cybercrime as a Service** – This is selling of cybercriminal services, techniques, and tools to be easily accessible on the dark web which includes malware distribution, ransomware as a service, stolen PII data etc.

Conclusion

While technology advancement is happening at never-before-seen pace it is also opening up new doors for fraudsters to exploit the same and become more innovative and sophisticated in committing frauds. As organizations continue to embrace, adapt, and evolve to provide the best of customer experience, more and more new methods of fraud are being worked upon in the dark web.

Technology is here to build and is also available for destruction and organizations need to be more resilient and vigilant than ever before to fight fire with fire. Hence it is imperative that organization lay equal emphasis to build fraud management solutions to not only detect fraud but prevent it in the first place which will ensure protecting their end customers as well as maintaining the brand value of the organization.

References

- The History and Evolution of Fraud | Fraud.com
- From Scam to Safe: The Evolution of Fraud Management Techniques | by grc viewpoint | Medium
- Four GEN AI fraud trends to watch in 2024 - Global Insights (experian.com)
- Generative Adversarial Network Definition | DeepAI
- Convolutional Neural Network Definition | DeepAI
- The Role of Generative AI in Fraud Detection: A Game-Changer | Oscilar
- Introduction To Autoencoders. A Brief Overview | by Abhijit Roy | Towards Data Science
- Top Fraud Trends for 2024 & How to Prevent Them (cybernewslive.com)
- Global Fraud Report 2023 (PDF) (cybersource.com)
- Generative AI Fraud: FraudGPT, WormGPT, and Beyond (ironscales.com)
- How Is AI Used in Fraud Detection? | NVIDIA Blog
- What is Retrieval-augmented generation (RAG) and its impact on fraud prevention | LinkedIn
- Unveiling the Forefront: Key Advantages of Leveraging Generative AI in Fraud Detection | LinkedIn

Author

Sumanth Dakshinamurthy is a Principal Consultant with over 20 years of experience in Quality Engineering and 15 plus years in Telecom Domain. He has conceptualized and built solutions in the Telco space leveraging AI/ML to enhance customer experience, self-healing solutions etc. His current focus is in the emerging Tech space where he is exploring new solution development across different industries leveraging Generative AI.

For more information, contact askus@infosys.com

Infosys®
Navigate your next