TATA CONSULTANCY SERVICES

Building on belief

Thwarting telecom fraudsters with artificial intelligence

Abstract

The telecom industry is the backbone of the world economy. Along with providing uninterrupted services to existing customers and catering to an ever-growing subscriber base, the onus of providing digital security to its patrons also falls squarely on the telecoms. However, the industry's vulnerability to fraud poses a significant and pervasive problem, besides resulting in a massive revenue drain.[1] According to the Communications Fraud Control Association 2019, the global telecom industry has reportedly suffered a loss of 28.3 billion a year on account of fraud i.e. 1.74% of its total annual revenue. In percentage terms, the increase in fraud loss is estimated to be 37%, when compared to their 2017 report.

As technology rapidly evolves, fraudsters are finding novel and innovative ways to perpetrate fraud, affecting both telcos and customers. As the current defenses to combat fraud fall short, the telecom industry urgently needs to adopt a futuristic approach to control and mitigate the same.[2]

This paper delves into the challenges faced by the telcos and explores some of the cutting-edge technologies they can deploy to safeguard against imminent threats and frauds.

Keeping their guard up

As challenging as it is to help curb fraud, the issues that telcos must be vigilant about include the following:

Novel techniques - Traditionally, International Revenue Share Fraud (IRSF) has been the most popular type of fraud. Although voice service-based, telecom revenue siphoning frauds are still at the forefront, fraudsters are shifting gears to directly target consumers by indulging in identity theft, using advanced tools to reduce traceability and culpability.[3],[4],[5],[6].

However, to fight fraud, Telcos continue to use obsolete rules based on past experiences. Today, the amount of data produced and the depth of analysis required have grown to unprecedented levels. Data is expected to reach telcos at lightning speed, and the average time per user interaction will reduce further.

---

[1] *FRAUD LOSS SURVEY;Nov 2019; https://cfca.org/wp-content/uploads/2021/02/CFCA-2019-Fraud-Loss-Survey.pdf; Accessed 01 Oct, 2021*

[2] *Financial crime and fraud in the age of cybersecurity; 01 Oct, 2019; www.mckinsey.com/business-functions/risk/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity#; Accessed 01 Oct, 2021*

[3] *https://www.raconteur.net/risk-management/fraud-destabilise-global-economies*

[4] *https://thepaypers.com/expert-opinion/the-changing-nature-of-fraud-in-telecommunications-industry--773807*

[5] *https://cfca.org/wp-content/uploads/2021/02/CFCA-2019-Fraud-Loss-Survey.pdf*

[6] *https://www.europol.europa.eu/publications-documents/cyber-telecom-crime-report-2019*

Focus on 'digital trust' - Since the Covid-19 pandemic, reliance on telecom networks has risen exponentially - be it for banking, schooling, remote work, streaming services for entertainment, or e-shopping. Further, customer's concerns about telcos upholding and explicitly demonstrating 'digital trust' to enable them to engage in business transactions in an unambiguously safe and secure, and reliable manner is now more important than ever.

Overcoming the odds

Below are some of the challenges that face the telecom industry:

Reliance on rule-based fraud detection systems - To fight fraud, most telcos predominantly continue to use a rule-based fraud detection approach, which is more reactive than predictive, given the short cycle times of transactions. Often, the alerts might reach the telco after an anomaly has already occurred. With the advent of 5G and edge computing, large volumes of data are exchanged bi-directionally between the telcos and customers almost instantaneously. With increasing volumes in communication supported by rapidly evolving technology, the process of operating solely through rule-based legacy systems is impractical, time-intensive and detrimental to customer experience in the new age.

Lack of customized solutions - Solutions for real-time fraud prediction, or lack thereof, and existing fraud control protocols need to be updated. Currently, existing solutions still follow a one-size-fits-all approach. They are usually designed and implemented in response to fraud instigations by known stimuli to define and update fraud controls, i.e. the same control set is applied across the customer base. As a result, there is a lack of personalized customer protection in addition to avoidable inconveniences.

The earlier a fraud alert reaches a telco decision-maker, the higher its value and relevance. Towards this, while machine learning (ML) technology is being employed to some extent by industry players, the full extent of its capabilities have not been exploited sufficiently, leaving untapped potential in the power of AI.

With criminals turning technology savvy, constantly researching potential vulnerabilities and developing fresh attack vectors, the use of AI to detect simple, fixed and known patterns is vastly inadequate.[7] Figure 1 below illustrates some of the recommended technology levers and their potential to combat fraudsters exploiting loopholes in hi-tech solutions.

[7] *https://www.capacitymedia.com/articles/3824627/battling-fraud-into-the-future*

Technology as a solution fix

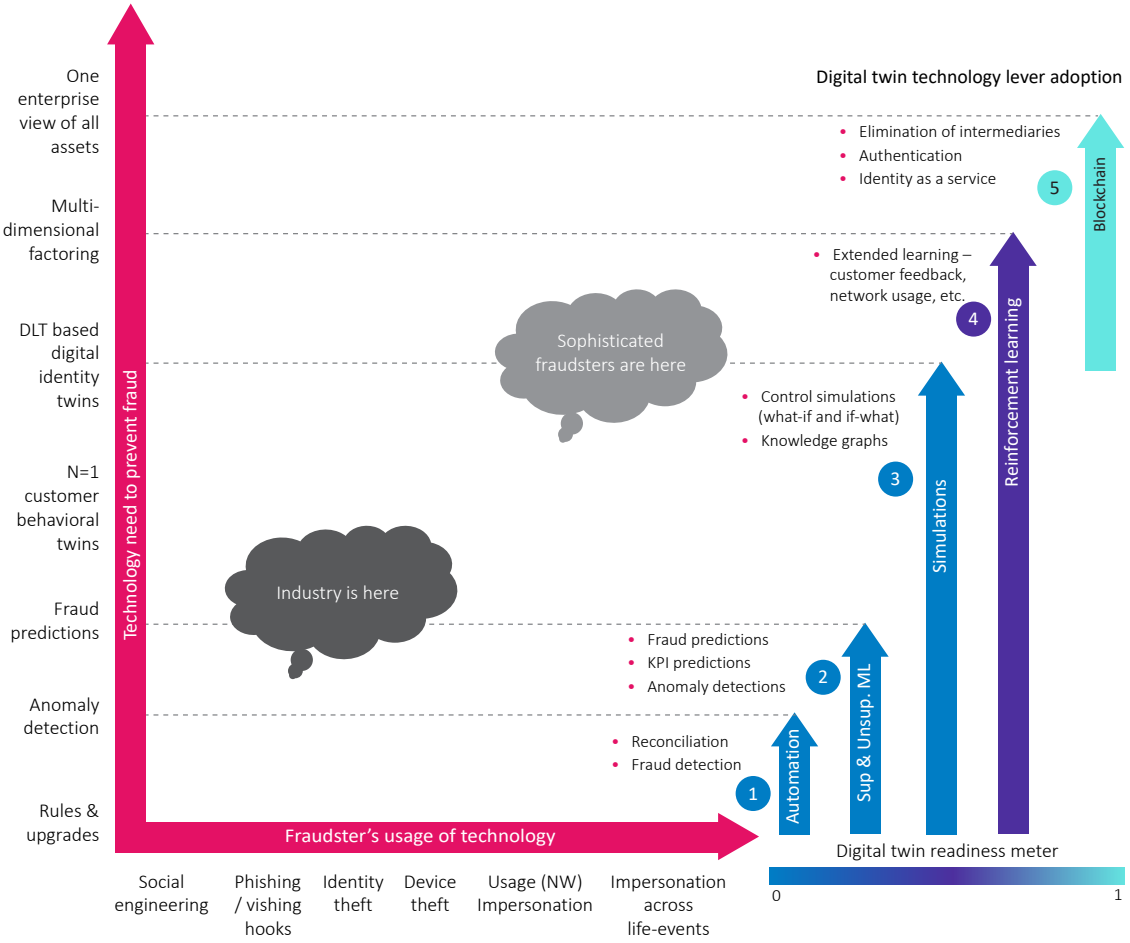

Figure 1: Technology usage evolution in fraud management

The techniques conventionally employed for fraud management broadly fall into two categories – fraud detection and, at a nascent stage, fraud prediction. In the former, fraudulent behavior is picked up by the fraud management system after a fraudster perpetrates fraud. In the latter, fraudulent behavior is anticipated before the event manifests. The core focus of both categories is that both methods keep the fraudster as the main focus. But, a revolutionary approach to combat modern-day fraud would be to shift focus from the fraudster to the potential victim. This can be done by predicting and modeling what makes the victim 'attractive' to the fraudster, which holds the key to effectively combating fraud.

Such models can be created for entities such as customers, products, agents, processes or /systems, physical equipment resources and so on, to gain insights and deeply understand specific protection requirements. These models can then be used to measure real-life entities' target-worthiness to the fraudster. With this intelligence, preemptive counter-measures to safeguard and protect potential victims, subjects, and media can be proactively placed to prevent future attacks, without the need for a "sacrificial lamb" (first victim) to trigger controls.

Promoting fraud control efficiencies: Controls can be tested with simulated fraud scenarios (analogous to fire drills). Control combinations can be compared and ranked based on impact predictions to key performance indicators (KPIs): both revenue assurance (e.g. revenue leakage) and beyond (e.g. customer satisfaction or new revenue potential).

For cases involving multiple intermediary parties such as roaming fraud, a blockchain-based solution could facilitate faster and unbreachable data, and value exchange, expediting fraud detection and system response times.[8],[9],[10].

Creating and updating fraud controls to regulate fraud detection and handling:

Fraud management has two facets – prediction of fraud occurrence and maintenance, creation and updates on fraud controls.

Conventional machine learning (ML) tools revolve around detecting known frauds using supervised learning and picking up on data anomalies using unsupervised learning techniques. After evaluating such occurrences, or upon a breach and alert, domain experts create fraud control rules. Although still in vogue, this makes the process reactive and labor-intensive as elucidated in figure 2 below.

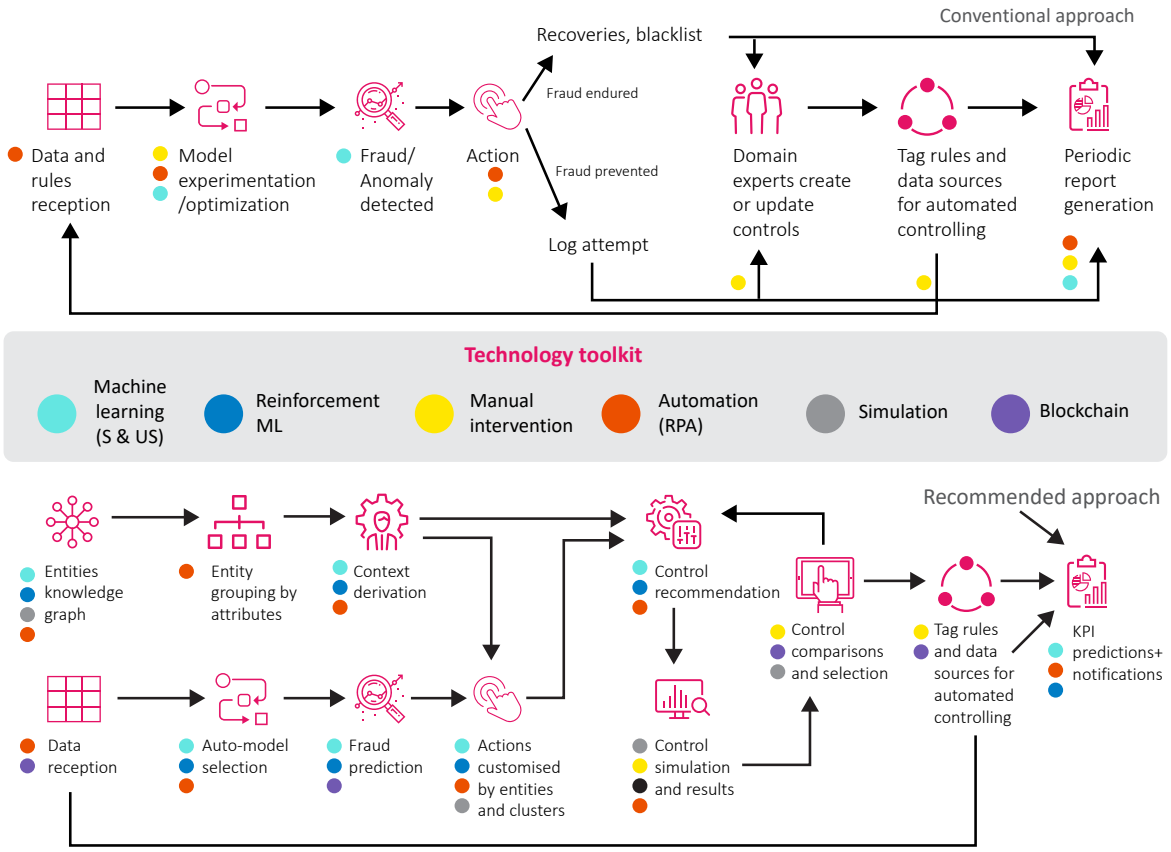

Figure 2: Comparative analysis of conventional versus recommended fraud control approaches

A more effective approach would be to have the data take dual divergent paths. One path can allow the data to stream into ML models to focus on the model selection for transactional fraud prediction and continual model training, as outlined above. The other path can be designed to derive the context to create or update 'digital twins,' and vulnerability profiles of entities involved in transactions.

These digital twins augment fraud mitigation by adding context to monitored transactions, thereby enhancing prediction speed and accuracy, while reducing dependence on data from each fraud

---

[8] *FRAUD LOSS SURVEY;Nov 2019; https://cfca.org/wp-content/uploads/2021/02/CFCA-2019-Fraud-Loss-Survey.pdf; Accessed 01 Oct, 2021*

[9] *Financial crime and fraud in the age of cybersecurity; 01 Oct, 2019; www.mckinsey.com/business-functions/risk/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity#; Accessed 01 Oct, 2021*

[10] *https://www.raconteur.net/risk-management/fraud-destabilise-global-economies*

prediction to gain knowledge on potential victims. Furthermore, in this path, these twins could become enablers for ML models to recommend new controls or updates to existing controls.

Decisions thus taken after simulation-based experimentation and evidence of outcomes, are launched and further measured for effectiveness in the real world. The differences (or lack thereof) between predicted outcomes and the actual outcomes provide vital inputs to ML models through a feedback loop created using reinforcement learning. As a result of these iterations, the accuracy of predictions further improves and ensures that the difference between the virtual world and the real world constantly diminish.

Investing in digital twin and simulation technology for improved outcomes

In the telecom industry, there is a constant trade-off between security and customer experience. Enhanced security measures entail process elongation, which adversely impacts customer experience and erodes the customer base. So, in their efforts to retain and attract more customers with quick and seamless experiences, telcos often tend to compromise on security. However, hyper-personalized strategies for customers based on individual risk profiles and modeling can help telcos pre-empt fraud while enhancing customer experience and expanding their customer footprint.

Simulation capabilities can help further evaluate the effectiveness and drawbacks of controls before launch. Controls can be evaluated against established risk taxonomies for broad range of business functions.

The following table illustrates the viable benefits of KPIs for various executives in a typical telecom organisation.[11]

Benefactor	Key performance indices (KPIs)
CFO, CRO	• Reduced revenue leakage • Increased revenue savings • Reduced mishap management costs (compensations, legal fees etc.) • Reduced legal implications • Lower residual risk (Risk mitigation)
CEO, CMO	• Improved NPS (heightened customer trust) • Reduced churn • Improved customer lifecycle valule (repeat buying) • Improved customer experience • Improved brand image
CFO, CRO	• Higher RAMM (Revenue Assurance Maturity Model - TM Forum Score) • Thought leadership and technologies prowess • Wider revenue assurance coverage
CEO, CMO	• Reduced process time • Reduced mean-time-to-detect and mean-time-to-prevent fraud • Operational efficiency (resources are preserved for legitimate transaction when fraudulent transactions are prevented)

[11] *https://www.capacitymedia.com/articles/3824627/battling-fraud-into-the-future*

The way forward

Today, the telecom industry is a unique amalgamation of multiple verticals. Consequently, the industry also inherits the intrinsic fraud risks associated with each vertical. Compared to traditional criminal modus operandi, telecom fraud has a widened scope and becomes a low-risk, yet lucrative alternative to traditional crime methods.

Across continents, collaboration, cooperation, and sharing of information is crucial to develop robust fraud control systems to thwart fraudsters. The rise of 5G and the evolution of new technology and anytime, anywhere connectivity will further fuel the growth of cyber-crime and telecom-led fraud. While telcos must continuously educate and inform their customers about the importance and methods of safeguarding their personal information and confidential data, they must also be proactive, invest in and develop dynamic controls and nimble processes that fraudsters will find hard to circumvent.

About the author

Agnetta Rebecca Ruskin, an electronics and communications engineer with a master's degree in international business, is part of TCS's Communications, Media and Technology group. She is a GTM lead for TCS TwinX, an enterprise digital twin platform with a unique combination of AI and TCS Research based simulation technologies. She owns the platform's fraud control module and is responsible for its concept-to-market activities. She has over five years of experience in innovative solution prototyping, sales and marketing, product ownership, client consulting and business analysis leadership for AI solution implementations.

TATA CONSULTANCY SERVICES

Awards and accolades

#1 IN CUSTOMER SATISFACTION 2020/21 EUROPE Whitelane Research

top EMPLOYER NORTH AMERICA 2021 CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

top EMPLOYER GLOBAL 2020 CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

ASIA'S OUTSTANDING COMPANIES POLL 2020 ASIAMONEY

STEVIE AWARDS 2020

CONGRATULATIONS CIO 100 WINNERS 2020

FinanceAsia ASIA'S BEST COMPANIES 2020

DIGITAL IMPACT AWARDS WINNER

CANADIAN HR AWARDS 2020

THE CIVIC 50 POINTS OF LIGHT

FTSE4Good

CDP DISCLOSURE INSIGHT ACTION

2020 Brand Finance® Awards
TOP 3 IT SERVICES BRAND

2020 Brand Finance® Awards
FASTEST GROWING IT SERVICES BRAND FOR THE DECADE 2010 - 2020

AWARDED Superbrands BRITAIN'S CHOICE 2020

AWARDED Superbrands AMERICA'S CHOICE 2020

Contact

For more information on Communications, Media & Technology visit https://www.tcs.com

Email: global.cmi@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is a purpose-led transformation partner to many of the world's largest businesses. For more than 50 years, it has been collaborating with clients and communities to build a greater future through innovation and collective knowledge. TCS offers an integrated portfolio of cognitive powered business, technology, and engineering services and solutions. The company's 500,000 consultants in 46 countries help empower individuals, enterprises, and societies to build on belief.

Visit **www.tcs.com** and follow TCS news **@TCS**.

Corporate Marketing | Design Services | M | 12 | 21