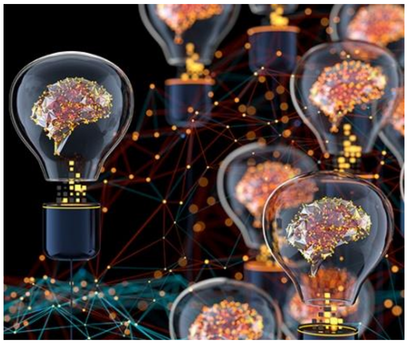
www.pipelinepub.com
Volume 18, Issue 8

The AI-First Approach to Fraud Detection and Prevention

By: Suresh Chintada



Fraud is a persistent nuisance for communications service providers (CSPs) across the globe, and unfortunately it just continues to grow in intensity.

The increasing use of sophisticated technologies by the fraudsters has resulted in a surge in the frequency as well as the intensity of telecom frauds. CSPs' digital transformation and the ever-increasing pervasiveness of the digital economy have only made it worse. The growing 5G ecosystem now is likely to make CSPs' ongoing battle with fraud even more important.

According to Communications Fraud Control Association's (CFCA) Fraud Loss Survey Report, 2021, the total telecom revenue loss due to fraud is estimated to be 2.22 percent of total revenue, or $39.89 billion. What is more worrying is that there has been a 28 percent increase in fraud losses when compared to 2019. Apart from revenue loss, fraud also results in loss of reputation and potentially even subscribers for CSPs.

The traditional rule-based fraud management systems are not enough to address the growing sophistication, frequency, and ferocity of telecom frauds, thus making it imperative for CSPs to rethink their fraud management measures and strategy.

Fraudsters' tactics have evolved over the years as the traffic on the communications networks continues to grow. The obsolete risk management systems are hardly geared to prevent or detect fraud. As a result, it has become more challenging for CSPs to detect fraud even as losses continue to mount for telcos in all geographies.

The growing sophistication of the fraudsters means that CSPs, who continue to use older and traditional fraud management systems, are on the back foot and are always trying to catch up with the modern methods used by the fraudsters.

CSPs can no longer depend on traditional fraud management systems because fraudsters are using innovative technologies to conduct fraud. In a way, fraudsters are taking advantage of the gaps in the weak and redundant traditional fraud management system to conduct frauds blatantly.

A key issue CSPs face is that the traditional rule-based fraud management systems are reactive in nature. This can be particularly problematic considering that 5G will significantly expand the number of protocols, applications, systems, and endpoints, leading to enhanced risks. It's imperative that with faster cloud adoption and a growing 5G ecosystem, fraud management needs to transform to be preventative and proactive.

Increasing technology and process complexity

One of the key reasons CSPs continue to struggle to catch up with the growing crimes is the increasing network complexity because of new technologies and the ever-increasing number of services they offer. Telecom service providers are no longer offering just vanilla voice and data connectivity. Mobile money and other fintech products, educational products, and gaming are just some of the new services provided by the telecom service providers. Furthermore, several service providers have started offering 5G-enabled augmented reality (AR), virtual reality (VR), and Industry 4.0 use cases. All this leads to a massive change in how telco business and operations are managed.

The operations are further complicated by the emergence of new business models, such as partner-led business models, API-led business models, compute-led business models, subscription-led business models and use-case-led business models, making traditional fraud systems deficient. The new use cases and business models will require integration with different types of platforms in which they are not just monitoring or evaluating data but also need to respond in real time.

In the 5G era, CSPs will need to collate and manage data in real time from several sources to proactively mitigate risks, thus making it critical to revamp their fraud management strategy. In addition, 5G will enable a greater number of deployed devices, which unfortunately provide a larger attack surface for fraudsters using Internet of Things (IoT) devices. According to CFCA Fraud Loss Survey Report 2021, 32 percent of CSPs expect to see an increase in 5G fraud because of protocols and the number of connected devices. The manual processes are not designed to manage the growing volume, variety, and velocity of data likely to be generated in the 5G era. According to OpenSignal, 5G users consume 2.7 times more data than 4G users.

As the services offered by telcos grow, the CSP partner ecosystem also records an increase. The growing ecosystem of the Internet of Things (IoT) especially poses a challenge for CSPs, as it brings to the fore different types of devices, partners, and service providers on one platform, thereby providing newer avenues for fraudsters to access the system. One weak link is enough for fraudsters to carry out a massive scam, significantly impacting CSPs' profitability.

Growing skill challenge

Faster adoption of the cloud and the growing 5G ecosystem mean that the risk management teams require new capabilities to deal with risks posed by new technologies and use cases that cut across several products and services.

CSPs' risk management teams need to be agile to continuously handle changes in the business. The teams should also have the ability to perform different data operations such as statistical analysis, behavioral analysis, protocol analysis, predictive analysis, and so on to capture risk-based insights from the data.

There is a greater need to upskill and increase data literacy within CSPs' risk management teams. This is crucial to gain the ability to deal with newer forms of data sets to address the evolving type of fraud—and also to ensure the successful implementation of risk mechanisms.

A key challenge faced by risk management teams, however, is the skills shortage. According to the Risk & Assurance Group 2021 Digital Trust Survey, finding skilled people is one of the critical challenges faced by CSPs in addressing growing fraud. This is likely to further grow with the 5G ecosystem, leading to an increase in the demand for these skills.

CSPs can partly address these challenges by using AI-powered automation. It is critical for the risk management teams to quickly scale up, enhance coverage and bring down the dependency on manual labor. This will also increase operational efficiency while freeing up resources for more strategic work.

Addressing new-age fraud with an AI-first approach

Amid growing fraud losses and the emergence of new challenges, CSPs stand to benefit by leveraging the capabilities of artificial intelligence (AI) and machine learning (ML) based systems to gain the required efficiencies to address new-age fraud. AI and ML hold tremendous potential for CSPs to not only bring down fraud-related losses but also to enhance the trust of their subscribers in their infrastructure.

An AI-powered fraud management system comes with capabilities to quickly identify and respond to suspicious activity. It can combine data, both structured and unstructured, from several data streams and make sense of it in real time to help telcos efficiently stop fraud before it negatively impacts their revenue and reputation.

In addition, AI and ML will be key proponents for handling changes in business scenarios and enabling risk management teams to be more agile. Another key advantage of an AI-based system is that it can collate both structured and unstructured data from multiple sources such as Kafka, pub-sub, APIs, and more, leading to faster detection of fraud and minimizing fraud run time.

Also, CSPs can further leverage AI and ML capabilities to make informed decisions if it is explainable, meaning that it provides complete clarity and visibility on how decisions are taken. Therefore, a fraud management system based on Explainable AI eliminates AI bias completely and provides transparency on how decisions are made.

Despite the potential, however, adoption of AI/ML-based fraud systems continues to be low. As per the CFCA Fraud Loss Survey Report 2021, 30 percent of the respondents are still using manual processes, while 28 percent use rules-based fraud management systems, and only 13 percent are leveraging AI and ML-based fraud management systems. The increasing sophistication of the frauds committed underlines that the methods being used by CSPs are not sufficient. Therefore, CSPs must adopt an AI-based approach to bring down fraud-related revenue loss.

The growing fraud losses of telcos coupled with the increasing level of sophistication of fraudsters means that CSPs must reexamine their fraud management strategy. It is time to adopt AI-first fraud management systems that use the latest technologies for both prevention and quick detection of fraud, thereby taking a more proactive—rather than reactive—approach to risk mitigation.

Fraud is a persistent nuisance for communications service providers (CSPs) across the globe, and unfortunately it just continues to grow in intensity.

The increasing use of sophisticated technologies by the fraudsters has resulted in a surge in the frequency as well as the intensity of telecom frauds. CSPs' digital transformation and the ever-increasing pervasiveness of the digital economy have only made it worse. The growing 5G ecosystem now is likely to make CSPs' ongoing battle with fraud even more important.

According to Communications Fraud Control Association's (CFCA) Fraud Loss Survey Report, 2021, the total telecom revenue loss due to fraud is estimated to be 2.22 percent of total revenue, or $39.89 billion. What is more worrying is that there has been a 28 percent increase in fraud losses when compared to 2019. Apart from revenue loss, fraud also results in loss of reputation and potentially even subscribers for CSPs.

The traditional rule-based fraud management systems are not enough to address the growing sophistication, frequency, and ferocity of telecom frauds, thus making it imperative for CSPs to rethink their fraud management measures and strategy.

Fraudsters' tactics have evolved over the years as the traffic on the communications networks continues to grow. The obsolete risk management systems are hardly geared to prevent or detect fraud. As a result, it has become more challenging for CSPs to detect fraud even as losses continue to mount for telcos in all geographies.

The growing sophistication of the fraudsters means that CSPs, who continue to use older and traditional fraud management systems, are on the back foot and are always trying to catch up with the modern methods used by the fraudsters.

CSPs can no longer depend on traditional fraud management systems because fraudsters are using innovative technologies to conduct fraud. In a way, fraudsters are taking advantage of the gaps in the weak and redundant traditional fraud management system to conduct frauds blatantly.

A key issue CSPs face is that the traditional rule-based fraud management systems are reactive in nature. This can be particularly problematic considering that 5G will significantly expand the number of protocols, applications, systems, and endpoints, leading to enhanced risks. It's imperative that with faster cloud adoption and a growing 5G ecosystem, fraud management needs to transform to be preventative and proactive.

Increasing technology and process complexity

One of the key reasons CSPs continue to struggle to catch up with the growing crimes is the increasing network complexity because of new technologies and the ever-increasing number of services they offer. Telecom service providers are no longer offering just vanilla voice and data connectivity. Mobile money and other fintech products, educational products, and gaming are just some of the new services provided by the telecom service providers. Furthermore, several service providers have started offering 5G-enabled augmented reality (AR), virtual reality (VR), and Industry 4.0 use cases. All this leads to a massive change in how telco business and operations are managed.

The operations are further complicated by the emergence of new business models, such as partner-led business models, API-led business models, compute-led business models, subscription-led business models and use-case-led business models, making traditional fraud systems deficient. The new use cases and business models will require integration with different types of platforms in which they are not just monitoring or evaluating data but also need to respond in real time.

In the 5G era, CSPs will need to collate and manage data in real time from several sources to proactively mitigate risks, thus making it critical to revamp their fraud management strategy. In addition, 5G will enable a greater number of deployed devices, which unfortunately provide a larger attack surface for fraudsters using Internet of Things (IoT) devices. According to CFCA Fraud Loss Survey Report 2021, 32 percent of CSPs expect to see an increase in 5G fraud because of protocols and the number of connected devices. The manual processes are not designed to manage the growing volume, variety, and velocity of data likely to be generated in the 5G era. According to OpenSignal, 5G users consume 2.7 times more data than 4G users.

As the services offered by telcos grow, the CSP partner ecosystem also records an increase. The growing ecosystem of the Internet of Things (IoT) especially poses a

challenge for CSPs, as it brings to the fore different types of devices, partners, and service providers on one platform, thereby providing newer avenues for fraudsters to access the system. One weak link is enough for fraudsters to carry out a massive scam, significantly impacting CSPs' profitability.

Growing skill challenge

Faster adoption of the cloud and the growing 5G ecosystem mean that the risk management teams require new capabilities to deal with risks posed by new technologies and use cases that cut across several products and services.

CSPs' risk management teams need to be agile to continuously handle changes in the business. The teams should also have the ability to perform different data operations such as statistical analysis, behavioral analysis, protocol analysis, predictive analysis, and so on to capture risk-based insights from the data.

There is a greater need to upskill and increase data literacy within CSPs' risk management teams. This is crucial to gain the ability to deal with newer forms of data sets to address the evolving type of fraud—and also to ensure the successful implementation of risk mechanisms.

A key challenge faced by risk management teams, however, is the skills shortage. According to the Risk & Assurance Group 2021 Digital Trust Survey, finding skilled people is one of the critical challenges faced by CSPs in addressing growing fraud. This is likely to further grow with the 5G ecosystem, leading to an increase in the demand for these skills.

CSPs can partly address these challenges by using AI-powered automation. It is critical for the risk management teams to quickly scale up, enhance coverage and bring down the dependency on manual labor. This will also increase operational efficiency while freeing up resources for more strategic work.

Addressing new-age fraud with an AI-first approach

Amid growing fraud losses and the emergence of new challenges, CSPs stand to benefit by leveraging the capabilities of artificial intelligence (AI) and machine learning (ML) based systems to gain the required efficiencies to address new-age fraud. AI and ML hold tremendous potential for CSPs to not only bring down fraud-related losses but also to enhance the trust of their subscribers in their infrastructure.

An AI-powered fraud management system comes with capabilities to quickly identify and respond to suspicious activity. It can combine data, both structured and unstructured, from several data streams and make sense of it in real time to help telcos efficiently stop fraud before it negatively impacts their revenue and reputation.

In addition, AI and ML will be key proponents for handling changes in business scenarios and enabling risk management teams to be more agile. Another key advantage of an AI-based system is that it can collate both structured and unstructured data from multiple sources such as Kafka, pub-sub, APIs, and more, leading to faster detection of fraud and minimizing fraud run time.

Also, CSPs can further leverage AI and ML capabilities to make informed decisions if it is explainable, meaning that it provides complete clarity and visibility on how decisions are taken.

Therefore, a fraud management system based on Explainable AI eliminates AI bias completely and provides transparency on how decisions are made.

Despite the potential, however, adoption of AI/ML-based fraud systems continues to be low. As per the CFCA Fraud Loss Survey Report 2021, 30 percent of the respondents are still using manual processes, while 28 percent use rules-based fraud management systems, and only 13 percent are leveraging AI and ML-based fraud management systems. The increasing sophistication of the frauds committed underlines that the methods being used by CSPs are not sufficient. Therefore, CSPs must adopt an AI-based approach to bring down fraud-related revenue loss.

The growing fraud losses of telcos coupled with the increasing level of sophistication of fraudsters means that CSPs must reexamine their fraud management strategy. It is time to adopt AI-first fraud management systems that use the latest technologies for both prevention and quick detection of fraud, thereby taking a more proactive—rather than reactive—approach to risk mitigation.