International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 12 Issue 3 ǁ March 2024 ǁ PP. 169-173

Fraud in Insurance Industry: Challenges and Opportunities

Khirod Chandra Panda
Principal Engineer
khirodpanda4bank@gmail.com

Abstract - *Fraud poses a significant challenge for insurance companies, often involving collaboration among fraudsters who assume various roles. To improve fraud detection accuracy, it's crucial for insurers to develop effective claim assessment systems. In this study, we introduce an investigative system based on bipartite networks, which illuminate the connections between individuals and accidents or vehicles and accidents. We establish filtering rules using probability models and evaluate methods for identifying communities within extensive networks. Additionally, we propose new alert metrics for detecting suspicious structures. To validate our approach, we apply it to real-world data from the Italian Antifraud Integrated Archive and compare our results with ongoing fraud investigations by judicial authorities. In the realm of insurance fraud detection, machine learning has garnered substantial interest. While supervised learning has been extensively studied for this purpose, the application of unsupervised learning remains relatively unexplored. This study aims to fill this gap by comparing the efficacy of supervised and unsupervised learning using proprietary insurance claim data. We also conduct a field experiment in collaboration with an insurance company to assess each approach's performance in identifying new fraudulent claims. Our findings indicate that unsupervised learning, particularly using isolation forests, can effectively detect insurance fraud. However, supervised learning also performs well, despite limited labeled fraud cases. Interestingly, the two approaches identify new fraudulent claims based on different input information. Therefore, we advocate for understanding supervised and unsupervised methods as complementary tools rather than substitutes in fraud detection implementation.*

Keywords *–Fraud, Machine Learning, Velocity Check, Rules, Supervised Learning,*

Date of Submission: 05-03-2024 Date of acceptance: 18-03-2024

I. Introduction

Fraud happens when people knowingly deceive others to gain an unfair advantage or deny someone what they're entitled to. In insurance fraud, legal action can be taken when certain conditions are met there must be an intent to defraud, meaning the person knowingly behaved deceitfully; an act must be committed, like giving false information to an insurer; and both the intent and the act must be present for a crime to be prosecuted. It's important to note that actual money loss isn't necessary for prosecution; what matters is the deceitful act and intent behind it. Providing wrong information when applying for insurance or filing a claim can lead to criminal charges.

Research shows how much insurance fraud costs American consumers. Study [1] [2] suggest it steals at least $308.6 billion every year and affects about 10% of property-casualty insurance losses. Medicare fraud alone costs $60 billion annually. This fraud is widespread across all types of insurance, with life insurance fraud at $74.7 billion, Medicare at $60 billion, property and casualty insurance at $45 billion, auto theft fraud at $7.4 billion, health insurance at $36.3 billion, and workers' compensation at $34 billion ($9 billion from premium fraud and $25 billion in claims fraud).

Further research [3] suggests, there are also legitimate companies selling products that look like insurance but aren't. For example, a company might sell health discount plans and call them insurance, even though they're not regulated insurance products. This can be confusing for consumers and highlights the need for clear information about insurance products.

The FBI's study [4] emphasizes the huge size of the insurance industry, which has over 7,000 companies and collects premiums totaling over $1 trillion annually. This large scale makes insurance fraud a big problem, providing many opportunities and strong incentives for illegal activities. The complex nature of insurance fraud shows the need for ongoing efforts to prevent and combat fraudulent behavior.

Study [5] suggests, more than one third of the 18 to 24 age group adults do not see insurance fraud as crime while over 96% of the people above 65 age group considers insurance as a crime.

Among various domains where fraud is a concern, Study [6] suggest, Device protection also is another niche area where industry is continuously getting spammed by fraudsters. Research [7] suggests, Auto insurers lose at least $29 billion a year in fraud.

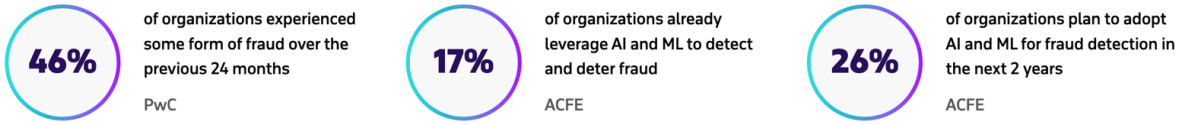

Fig 1 Machine learning in fraud detection: trends and stats

II. Literature Review

Detecting and preventing fraud is a significant challenge faced by both consumers and businesses of all sizes. As technology evolves, fraudsters continually develop more sophisticated methods to commit fraud, making it increasingly difficult to detect and prevent fraudulent activities. These fraudsters are driven by various motivations, including financial gain and personal gratification.

For organizations dealing with large volumes of data, such as those in the financial sector or e-commerce industry, manually identifying fraudulent transactions is not feasible. It is crucial to leverage automated processes and advanced technologies, such as artificial intelligence and machine learning, to analyze vast amounts of data and detect patterns indicative of fraudulent behavior.

These automated systems can examine multiple data points, including transaction history, user behavior, and geographic location, to assess the likelihood of fraud. By using algorithms to analyze these data points, organizations can quickly identify suspicious transactions and take appropriate action to prevent financial losses and protect their customers.

Implementing these automated fraud detection systems requires ongoing monitoring and adjustment to adapt to evolving fraud tactics. However, with the right technology and strategies in place, organizations can significantly reduce the risk of fraud and protect both their assets and their customers.

In fraud prevention, having access to a wide range of data points is crucial for making accurate decisions. The more data points you have, the better you can assess the risk associated with an account or transaction. These data points can include various types of information, such as user behavior, transaction history, device information, and more. By analyzing these data points, fraud prevention systems can identify patterns and anomalies that may indicate fraudulent activity.

Study [8] Having numerous data points allows fraud prevention systems to screen risky accounts effectively without needing to rely on connections with other users. This is important because not all fraudulent activities are linked to other users or accounts. Sometimes, a single data point, such as a suspicious IP address or unusual transaction pattern, can be enough to flag an account for further investigation.

For example, a fraud prevention system may use browser hash or ID to track and identify potentially fraudulent activity. This method generates a unique identifier based on the user's browser, operating system, device, and network information. By blacklisting browser hashes associated with fraudulent activity, the system can prevent users from logging in with fake IDs or engaging in scams.

While rules and blacklists based on single data points can be effective, they are not always the most scalable or efficient solution. As fraudsters continue to evolve their tactics, fraud prevention systems must also adapt by incorporating new data points and more sophisticated algorithms to stay ahead of fraudulent activity.

The COVID-19 pandemic has had a profound impact on the fraud detection and prevention market, reshaping the landscape and presenting new challenges and opportunities. One significant effect has been the increase in fraudulent activities, driven by the vulnerabilities and disruptions caused by the pandemic. Fraudsters have seized upon the chaos and uncertainty to perpetrate scams and schemes, including phishing attacks, identity theft, and financial fraud.

The pandemic has also heightened the complexity of fraud schemes, as fraudsters adapt to changing circumstances and exploit new vulnerabilities. For example, the shift to remote work and online transactions has

created new opportunities for fraud, requiring organizations to be more vigilant and proactive in their fraud detection efforts.

In response to these challenges, organizations have increasingly turned to advanced analytics, artificial intelligence, and machine learning to enhance their fraud detection capabilities. These technologies offer the ability to analyze large volumes of data quickly and accurately, enabling organizations to detect and respond to fraud more effectively.

Overall, the COVID-19 pandemic has underscored the importance of robust fraud detection and prevention measures. It has highlighted the need for organizations to invest in advanced technologies and proactive strategies to protect themselves and their customers from the growing threat of fraud.

Fig 2 Stages of Detection Process

III. Opportunities In Fraud Detection

3.1 Fine Tuning fraud detection strategy

3.1.1 Adding AI and ML to workflow.

Data is an integral part of detecting fraud. The more relevant data sets we have it becomes easier to find a pattern and flag a fraud. It is more than often easy to say than done.

The advancement in Machine learning helps in more sophisticated analysis of patterns and behaviors. Machine learning-based fraud detection systems rely on ML algorithms that can be trained with historical data on past fraudulent or legitimate activities to autonomously identify the characteristic patterns of these events and recognize them once they recur. For Machine learning algorithm to work it needs a data set to train upon. organizations must use and manage multiple sources of data (both structured and unstructured). Often because of the nature of the applications in its entirety, the data we get is not in. a standard format. So, it becomes imperative to first clean the data and transform the data to create a training data set to apply to a machine learning algorithm.

Achieving success in machine learning for fraud detection does not rely on a single algorithm or approach. Instead, it involves experimenting with various machine learning methods, exploring different variations, and testing them across diverse datasets. A proficient data scientist requires a diverse toolkit comprising both supervised and unsupervised methods, alongside a range of feature engineering techniques. Moreover, there is a creative element or "art" to machine learning in fraud detection. This involves innovatively applying fraud analytics, such as integrating multiple supervised and unsupervised machine learning methods within a single system, to enhance effectiveness beyond the capabilities of any individual method alone.

3.2. Improve investigation efficiency with intelligent case management.

The initial adoption of artificial intelligence (AI) in the context of fraud detection and financial crimes investigation is primarily focused on streamlining manual processes to reduce operational costs while enhancing efficiency. The goal is to free up investigators from mundane tasks that can be automated, allowing them to focus their expertise and attention on more complex and strategic aspects of their work.

An advanced analytics-driven alert and case management solution plays a pivotal role in this automation process. By providing a comprehensive view of data, this solution can automatically prioritize cases based on predefined criteria, recommend investigative steps, and expedite the resolution of straightforward cases. Additionally, it can enhance alerts with relevant details about associated customers, accounts, or beneficiaries, enabling investigators to gain deeper insights into potentially fraudulent activities.

Moreover, the solution intelligently retrieves and consolidates data from various internal databases or third-party sources, eliminating the need for manual data retrieval and aggregation. This capability not only

saves time but also ensures that investigators have access to all relevant information in a timely manner. Furthermore, the data is presented in intuitive visualizations on a single screen, making it easier for investigators to identify patterns, trends, and anomalies.

Another significant feature of the solution is its ability to automate the preparation of suspicious activity alerts (SARs) for electronic filing, where applicable. By auto-populating SARs with relevant information and ensuring compliance with regulatory requirements, the solution facilitates seamless reporting of suspicious activities to regulatory authorities.

In summary, the adoption of AI-driven solutions in fraud detection and financial crimes investigation aims to optimize operational efficiency, enhance decision-making capabilities, and ensure compliance with regulatory standards. By automating manual processes and leveraging advanced analytics, organizations can effectively combat fraudulent activities while minimizing operational costs and maximizing the productivity of their investigative teams.

3.3 Velocity Check

Velocity checks are an important aspect of fraud detection and are often used in conjunction with machine learning techniques. Velocity checks look at the rate at which certain events occur,

Research [9] suggest, Time is the key element in velocity-based fraud detection. In fraud detection, a velocity rule or filter is a mechanism employed to assess a user's behavior based on a combination of specific data points and timeframes. The purpose of applying velocity rules is to monitor the frequency and pattern of activities conducted by a user within a given period and identify any anomalies or suspicious behavior.

, within specific timeframes. For example, a velocity rule may specify that if a user attempts to make more than five transactions within a one-hour period, it should trigger a flag for further investigation.

By analyzing the user's behavior against these predefined rules, organizations can effectively detect potentially fraudulent activities and take appropriate actions to mitigate risks. If a user's behavior exceeds the thresholds defined in the velocity rules, it may indicate fraudulent behavior, such as account takeover or unauthorized access, prompting the system to flag the activity for manual review or intervention.

Overall, velocity rules play a crucial role in fraud detection by enabling organizations to monitor and analyze user behavior in real-time, allowing them to identify and respond to suspicious activities promptly.

Overall, velocity rules play a crucial role in fraud detection by enabling organizations to monitor and analyze user behavior in real-time, allowing them to identify and respond to suspicious activities promptly. These rules help enhance the accuracy and efficiency of fraud detection processes, ultimately safeguarding organizations, and their customers from fraudulent activities.

Velocity checking in the context of fraud prevention enables:

- Enhanced comprehension of user and fraudster conduct
- Enhanced fingerprinting
- Enhanced identification of fraud networks
- Enhanced awareness of threats and trends in threats
- More accurate and effective fraud detection
- Prevention of more sophisticated fraud schemes

IV. Conclusion

Given the economic significance of fraud prevention, it is imperative for insurance firms to establish streamlined and efficient procedures for uncovering fraudulent claims. This not only serves the financial interests of insurance companies but also results in reduced insurance premiums for honest policyholders. While existing literature has predominantly focused on evaluating supervised learning methods for identifying insurance fraud, these methods come with inherent limitations. Typically, there are minimal labeled instances available, and novel fraud patterns may go undetected. In contrast, unsupervised learning, particularly anomaly detection, offers potential solutions to these challenges. Despite its applicability in various fraud detection domains, research on employing unsupervised learning techniques for detecting insurance fraud remains limited.

Furthermore, there is a scarcity of empirical evidence to aid decision-making regarding the choice between supervised and unsupervised learning methods in insurance fraud detection. Given insurers' keen interest in identifying new instances of fraud, it is crucial to explore both observational and non-observational

data to discern the distinctions between supervised and unsupervised learning approaches in this domain. For instance, while supervised learning may benefit from a more comprehensive detection of partially known patterns, unsupervised learning could excel in identifying novel patterns previously unseen in the data.

References

[1] Coalition Against Insurance Fraud. (2023, June 20). Fraud Stats - Available. https://insurancefraud.org/fraud-stats/

[2] Insurance fraud. (n.d.). NAIC. Available. https://content.naic.org/article/consumer-insight-insurance-fraud

[3] Scam Glossary. (n.d.). Federal Communications Commission. Available. https://www.fcc.gov/scam-glossary

[4] Insurance fraud. (2020, September 15). Federal Bureau of Investigation. https://www.fbi.gov/stats-services/publications/insurance-fraud

[5] Coalition Against Insurance Fraud. (2024, February 3). WHO ME WEBINAR [Video]. Accessed: Feb 10, 2024. [Online Video] Available. https://vimeo.com/857908297?share=copy

[6] Barber, Z. (2023, May 9). The future of device Insurance Fraud - Phronesis. Phronesis Technologies Limited. Available https://phronesis.net/solutions-to-phone-insurance-fraud/

[7] Background on: Insurance fraud | III. (n.d.). Available https://www.iii.org/article/background-on-insurance-fraud

[8] Tanant, F., & Tanant, F. (2023, November 29). Spotting customer connections thanks to AI fraud prevention engines. SEON. Available https://seon.io/resources/how-to-spot-hidden-customer-connections-through-ai/

[9] What are velocity checks & velocity rules? | SEON. (2023, November 22). SEON. Available: https://seon.io/resources/dictionary/velocity-check/