# Streaming Risk Scoring and Behavioural Pattern Recognition: A Real-Time Machine Learning Architecture for Insurance Fraud Risk Assessment

*Dr. Jorge Murillo, Professor of Industrial Engineering, Universidad de Antioquia (Colombia)*

## 1. Introduction

Artificial intelligence (AI) has a valuable role to play in the detection and prevention of insurance fraud. This is especially important because insurance fraud can cause substantial financial losses. In the United States alone, fraudulent claims amount to $80 billion annually, and experts estimate that the problem is even more serious for insurance companies in the European Union. Especially in the case of non-life insurance, insurance fraud prevention and detection are gaining in importance. As many cases of fraud are hard to prove, it is crucial to evaluate the probability of a particular claim being fraudulent. This chapter shows how real-time AI can be used in this sector and how legislative changes to some European Union non-life policies can potentially make the data available for modeling in latency rejection insurers.

The most advanced non-life insurers in the European Union often apply non-AI-oriented scoring models in order to analyze the risk. Latency scoring models are based on various kinds of indicators, including, for example, socio-demographic indicators, indicators for particular areas, etc. In the case of car insurance, commonly used latency scoring indicators include the marital status of the person insured, their gender, their age, the number of accidents over the past two to five years, and so forth. While this method is very effective in the prevention of non-life fraud, it also has many limitations. These traditional scoring methods are either too slow, or they violate the GDPR with their "fake reasons." In the future, it will be possible to use the numerous combinations of various versions of one picture of a particular face to anticipate fraud or financial loss from the images of the individuals' faces who are going to take a selfie.

### 1.1. Background and Significance

1. Insurance fraud is as old as insurance itself and is practiced worldwide. Insurance fraud costs domestic Australian companies in the general insurance industry billions of dollars annually. Insurance fraudsters are very sophisticated criminals who manage to avoid detection time and time again, or prefer to risk detection and conviction. Fraudulent attacks have grown substantially over the years as fraudsters gather and choose more confidential data to use for political or financial gain. Since fraud detections are inconsistent and remove their proceeds from the insurance company, they have both direct and indirect detrimental consequences. Consequently, according to shareholders, executives, and clients, the general insurance industry is under pressure to strengthen its capacity to assess the risk of fraud. Insurance agencies must develop strategies to react to these threatening tactics, especially because they have broadened their function to offer a range of new pricing models with improved service scope.

In order to warn organizations of emerging fraudulent behavior, numerous alerting and adaptive models have been introduced, but they have indicated a number of limitations such as patient sampling. Techniques that are focused on highly scalable, real-time information validation and respond to the changing fraud landscape are what's next. Because of the new production knowledge about predictive risk data mining, artificial intelligence algorithms have now emerged as an effective means of providing complex fraud analysis. The growth of artificial intelligence in finance has been rapid as a solution for real-time information analysis by businesses including insurance providers. The fraud hazard must be discovered or the insurance company can experience detrimental results.

### 1.2. Research Objectives

The primary objective of the research is to evaluate the effectiveness of AI-based applications concerning real-time fraud detection in the insurance setting. The purpose is to gain insight into whether the adoption of AI-driven solutions is beneficial for the insurance sector in terms of cost reduction and detection accuracy. Our second purpose is to explore any constraints current industry practices might face within the field of cleaning data. Special attention is focused on how the present practices adopted by insurance companies can pose a legitimate challenge for AI software, which has not been acknowledged in previous literature. In light of this purpose, three research questions

were identified: What are the advantages and potential benefits of adopting AI-driven systems compared to the already existing practices? Are there any constraints that the adoption of AI-driven solutions can face? Which industry practices are potentially posing constraints in adopting AI-driven software? To answer the research questions and the aim of this study, an empirical analysis was developed using real-time insurance claims data. Different models were developed to assess and compare industry practices used for detecting fraud risk with the results provided by various machine learning techniques, ruling out the most promising ones in the context of fraud detection systems in the insurance field. Proposed performance indices will be measured and discussed to illustrate the most promising alternatives to the current industry practices.

**2. Insurance Fraud Risk Assessment**

Insurance fraud is a serious and growing problem globally, and insurance companies lose over 10% of their income to fraud annually. Despite these astonishing figures, just about 10% of the frauds are detected each year. In some insurance segments, such as automobile and health insurance, some countries have seen fraud rates radically exceeding the loss ratio of 100%. There are several reasons why insurance fraud is so widespread: First, insurance products are sold over the counter, and both smaller and larger claims can offer healthy returns to the policyholder, who is also in perfect control of the size of the payout. Additionally, acceptance of unfair behavior is high among the public, especially since this touches upon products that are not complex and represent less dramatic crimes. Furthermore, advances in digital technology make it easier for individuals to manipulate claims applications, leading to increased fraud. Some proponents also argue that vast economic inequities have contributed to the proliferation of fraud as a reaction.

The general reasons for insurance fraud have to do with economic incentives, opportunity, and rationalization. Psychological impulses such as greed and envy can also play a role. The ideal countermeasure is to devise ways to limit all three of these potential causes. Insurance Fraud Risk (IFR) can be understood as a function of four main drivers: the size of claims, frequency of claims, program design, and claim administration. In other words, the assessment revolves around both the exposure of the underlying asset to damage and the extent to which the financial incentive exists to

commit fraud. In this study, we are focusing on the IFR linked to size as well as administrative fraud based on the claim process.

### 2.1. Challenges in Traditional Approaches

Historically, insurance firms have relied on manual or rule-based models for identifying fraud, which is slow or impossible to update to meet evolving threats. This approach means that organizations fail to see new threats in a typical year, as new fraud trends take off faster than firms can adapt. Problematically, most fraud detection systems and processes rely almost exclusively on historical fraud and loss data. In the months or years that it often takes to update a traditional solution, this historical data can become irrelevant, providing outdated risk assessments. This hinders insurance firms' capacity to understand and quickly identify the current fraud threats that they and their customers face. Organizations pay higher operational costs when they utilize manual labor for fraud investigations. In turn, this reduces the overall scalability of their business, constraining progress, profitability, and innovation.

Traditional approaches can take days, weeks, or even months to identify that a fraudulent activity has occurred, and longer still to figure out what has happened. Real-time AI-driven technologies, however, can analyze a vast range of technologies in real-time, taking each claim in the network and deciding whether it is likely to be fraudulent, likely to contain elements of fraud, or likely to be non-fraudulent.

### 2.2. Importance of Real-Time Solutions

Investigation and fraud are rampant across modern-day insurance activities. Despite the existence of various anti-fraud measures, sophisticated and intricate deception and corruption activities are on the rise. Fraud risk assessment of insurance policies is an important aspect of insurance fraud prevention. Traditional methods of payer image, claimant characteristics, loss features, etc., can help reveal a great deal of fraudulent data. The primary disadvantage of these methods, however, is that they often provide timely information about the fraud that has already occurred. Therefore, there is a need for real-time solutions that can analyze the input data and quickly determine whether a current activity is suspicious so that preventive measures can be taken if necessary.

Real-time solutions can be particularly beneficial in the event of ongoing surveillance of a single coverage or operation (e.g., a typically unusual decline in marketing and

distribution, or unjust practices in the review process). They may also be modified to provide exceptions about general input or input from certain insurance firms or operations. Turning non-real-time solutions into real-time solutions. Incorporating machine learning and knowledge of advanced situations may build a real-world service for risk assessment for fraud in insurance.

By comparing the insurance real world in cost savings, real-time solutions grant firms the chance to act proactively to inhibit scams that provide detection. Finally, insurance firms value quick access to actionable knowledge through real-time services to carry out detailed monitoring and effectively make decisions. Audits often demonstrate people's attitudes and engagement with enhanced consumer service, business values, and long-term trust. Predictive analytics options allow insurance firms to adjust their underwriting and pricing to the estimated probability of fraud. If this estimator depends on current data, insurance firms will use this knowledge to adjust rates as much as possible based on the current risk. Moreover, such rates will represent the fraud assessment approach. The amount of risk used to set premiums would indirectly penalize the lower risk of providing discounted scholarships for genuine customers.

**3. Machine Learning in Insurance Fraud Detection**

Machine learning lies at the heart of artificial intelligence. AI technologies are processing large volumes of data, bringing an entirely new dimension for understanding the different key trends and influencing factors, beyond what the human brain could ever digest. This is powerful as, with such an approach, insurance companies can have a much better understanding of the benefits and costs in the future for each customer, making the market more efficient and customers loyal while increasing profitability for insurance companies. There are multiple advanced machine learning approaches that help fight against fraudsters as they use data of different types coming from various sources to detect the existence of fraud, whereas three are of particular relevance in the insurance sector: support vector machines, neural networks, and ensemble models. Neural networks, as an underlying model for deep learning, have been found to be suitable for detecting fraud using telematics data in car insurance.

The most accurate models are those that combine known or well-performing prediction algorithms and use a diversified test dataset to make a decision based on their predictions, known as adaptive learning systems. To illustrate the importance of the

diversified test data, it was found that both random forest and extreme gradient boosting could be used as ensemble-based intelligent decision support systems for the insurance industry. However, when evaluating such models, it is important to bear in mind that the quality of a model is directly dependent on the quality of the test dataset. Consequently, when low performance metrics are obtained, it is as important to consider whether a model was trained with good quality test datasets to avoid misleading conclusions about its usefulness. Such analytical tools integrated on a real-time basis with existing transversal activities like fraud funds, internal fraud, and real-time sanctions checks cover an insurance-specific process more holistically and help facilitate organizational objectives while providing 'in-time' information to decision makers.

### 3.1. Overview of Machine Learning Techniques

In the context of fraud detection, various models can be used for risk assessment. Machine learning models can be categorized into supervised, semi-supervised, unsupervised, and reinforcement learning. Supervised models require labeled data for the training stage. For the validation or testing stages, model accuracy can be improved by enriching data. Semi-supervised models use both labeled and unlabeled data for training, while unsupervised methods work with unlabeled data to expect output features that describe the input data well. Reinforcement learning models use unlabeled examples of input data but rely heavily on feedback from the environment.

Different types of fraud can be detected using various machine learning theories. While in some cases data is available, in others it is not. In many cases, data availability is skewed, which means the number of fraud samples is significantly less than the number of genuine samples. Manually designed features can improve the accuracy of fraud detection models. Fraud detection systems based on neural networks are also effective when the model can be trained on static data, or when the concept of fraudulent behavior does not change abruptly. In cases of outliers, novelty, and unknown frauds, deep learning models provide additional flexibility to tune inputs to best represent data and highlight the data's potential for fraudulent behavior. The Random Forest model is good for situations where there are many missing values because it only uses those features that are relevant for predicting the class of activity. With the Random Forest

model, less human intervention is required for feature validation, which makes an insurer-independent system faster and provides real-time risk assessment.

### 3.2. Applications in Fraud Detection

As of now, there are no publicly available results of fraud detection cases using real-time artificial intelligence solutions designed by KASKO GmbH. However, due to the commonality of fraud detection as an exemplary case for predictive analytics in the insurance value chain, we would like to give an example.

Case studies for fraud detection. There are various case studies on the usage of machine learning or predictive analytics in the practice of fraud detection in ISC, e.g., where British United Provident Association Ltd applied a fraud framework for health insurance and saved £3.8 million, and Kocaeli University where a number of decision trees, ROC-CHAID, and SVM models were compared on an insurance claim fraud prediction case. A webinar cites a case study with 'a well-known US insurance company' effectively using predictive analytics in fraud prevention.

In a white paper, some collaborative fraud prevention actions are described, elaborating various insurance organizations' approaches to data sharing and model building. There are various case studies from work around fraud prevention in the banking and insurance sector. With law enforcement, recently a solution was developed to help investigators identify relationships, so criminal enterprises can be dismantled with computational techniques. In collaboration with major insurance companies, a sophisticated, industry-wide insurance fraud network is developed and operated to identify and refer cases of suspected fraudulent claims to local company bureaus for investigations. And this with significant success; not only did P&Cs on average double their incident referral rates, but they also had significant returns on investment. Another well-known provider of fraud detection systems is a company that provides security-driven claims solutions for the insurance industry operating in Thailand and Singapore. They currently work with 10 insurance companies and investigate a total of 300-400 cases per day.

## 4. Real-Time AI Solutions

4. Real-Time AI Solutions

In the past, static rule-based engines and AI application programs came into action only after fraudulent activities had been detected with some time lag. But today, Real-Time AI Solutions carry this alert function into the future before any activities could turn into fraud. AI Real-Time Solutions contain new and future procedures, services, and subsequent decision methodologies based on AI technologies. The AI Real-Time Solutions analyze and act upon the instantiation of dynamically changing data in data streams and apply the mathematically based detections of correlations and similarities in such dynamic and complex high-dimensional data.

Many AI Solutions analyze historical data to issue predictions. These are nearly static and non-real-time AI systems and have no or just time-lag response. On the contrary, Real-Time AI Solutions have instantaneous detection capabilities to analyze the structured, semi- or non-structured data streams at rest, in motion for detections from batches, online, or standardized interfaces. A new focus of the Real-Time Solutions is instant response mechanisms realized in the technical control room that do not analyze data in a siloed way but consider the whole system of system interaction with the intended, unintended, involuntary, negative feedback loop interactions.

**4.1. Key Components and Architecture**

With the five essential components in place and integrated, a real-time solution can be installed end-to-end. The deployment of the real-time solution spans multiple technological layers. At the very foundation of the deployment is the cluster of hardware that will manage business-specific inputs. Initially, the data is streamed to relevant hubs in the cloud-compute farms where network resources or data handling can be allocated to the incoming data streams to meet desired quality of service capabilities. Meanwhile, additional data storage can be provisioned based upon real-time cluster implementation and associated requirements, ensuring that there is no single point of failure. Atop the hardware deployments is the requisite software to handle networking traffic and patterns, ensuring that load balancing and data distribution are effectively segmented into the different tiers. The real-time clusters operate within these architectures using big data methodology, ensuring that storage is always landing on distributed storage, with parallel processing methods and techniques for stream processing being applied. As our storage environments become larger than memory scenarios, more rapid and efficient methods are devised for data selection. This

is necessary as, with real-time data, which is usually very large, combined with high stream rates, there is often a need for random or batch-based model applications within a very short time domain.

The security and permissioning framework, including tokenization, is used as pathways, and access to queries is thus available up to a 90-day window time period. Indeed, analytics applications underpin machine learning predictive models operating to produce the outputs, while scoring layers ultimately produce qualitative and quantitative scores and rankings. The above end-to-end deployments and architectures are real-time solutions used to help integration technologies and practices. The detection offers a simple way through real-time credit scoring, ranking, and risk assessment interface for insurers to seamlessly identify premium leakage. The collaboration of these various components results in the end-to-end installation that helps integration technologies. From our high-level analysis of the processes in real-time fraud risk assessment, we, however, see the need to approach operational integration from a broad basis, which includes the following: getting real-time signals from insurers in case of fraud, extending analytics life cycles, and operationalizing analytics into real-time to support business innovations. Evaluations from our solution determine if the integrated components produce integrated outcomes. Keep the simple interface at the front end for the insurance professionals and experts.

### 4.2. Integration with Insurance Systems

Real-time AI solutions must be in line with the current systems and software implemented in the insurance company. For insurance companies, it is necessary to obtain a smooth data flow from real-time AI solutions to existing platforms, both for assessing the mid-process risk of high-value objects and for assessing vehicle and home insurance fraud. It is essential to have a single database with the most up-to-date information on risk assessment from previous years that can be easily and quickly retrieved within any traditional system for data and risk management. Implementation is not limited to software, but often also encompasses hardware, education, and restructuring of the company's workflow. Available solutions are based on avoiding mass delays during an upgrade. The challenges of integrating a real-time AI system with existing systems are associated with increased technological demands on the organization, particularly as competitors accelerate the adoption of technology that can

lead to data overload. The major attraction, however, is time savings, as organizations do not need to wait for existing systems to be upgraded.

Disruptors of long-term solutions can be used very creatively by partners, taking advantage of their specific business processes or employee-user skills to create value. The companies' approaches are also similar: provide the partners with a system that provides access via the application programming interface, internet standards, and best business practices in terms of ethics, data protection legislation, and fraud prevention. When integrating systems, it is important to remember that insurance companies use a mix of older mainframe and client-server systems and the latest cloud-computing models. When integrating AI-driven fraud detection with various systems, these commercial models and their underlying technology can be very complex and varied. To connect two systems that are developed in very different environments, an API offers a relatively simple way to integrate them, using a universal data standard. As part of the product development process, AI manipulation software pulls key data out of the system to share with the fraud detection AI using an API. A brand-new application interface allows insurance companies to undergo a transformation. Real-time AI detects the highest possible fraudulent threshold. In this setting, the handle has minimal disruptive data-entry requirements until it is adopted within the rating systems, resulting in its widespread usage. Success is influenced, in equal measure, by collaboration with stakeholders. When different divisions do not interact or when organizations are built around 'silos', effective fraud integration becomes a 'pipe dream'. Regarding a collaborative standard at all levels of operation, the key to successful real-time AI integration is engaging all levels of the organization. Several concerned IT stakeholders also attempted to impair a last-in-class solution, but the proof of fraudulent discrimination shaped an easy choice for everyone. Application and system interface, step by step, is available in the next section as a case study solution.

**5. Case Studies and Applications**

Case studies and various field applications reveal, thanks to practical implementations, the strengths but also the limits of real-time AI fraud solutions. They cover various fields and illegal practices, different industries, and different types of offers, whether related to basic treatment alone or to remote treatment supplemented by additional AI-controlled offers. They help assess the real operational benefits associated with these new fraud

management solutions. Above all, they illustrate the dynamics through the evolution of a proper fraud culture among professionals in fraud risk management and guarantee for professionals in AI techniques.

They have succeeded in reducing the fraud rate, detecting it faster and earlier, effectively integrating AI techniques into new or existing business systems, and deploying their implementation when the scale of the insertion of real-time AI within the framework of the organizational project is compatible with market, technological, legal requirements, and corporate strategic orientations. They constitute practical examples that are consistent with practical needs and reassure professionals from other organizations to build their own applications. In summary, technical teams and insurance professionals engage in shared learning through experimentation and implementation. They adapt to the complexity of human behavior, whether that behavior is honest or dishonest. In any case, case studies and various field applications can significantly contribute to the professionalization of fraud risk management in companies or among inter-professionals in clear breakthrough scenarios that affect the organizations of insurance professionals and mutuals.

**5.1. Success Stories in the Industry**

Success Story No. 1: Employers use AI to reduce their claims fraud loss by 2% of their premium. "The technology implementation took a year and involved close collaboration between Employers' fraud investigations, IT, claims adjusting, solutions architect, business analytics, and business process management teams, all representing an innovative blend of key company functions. 'The blending of these operations allowed for an integrated approach to problem solving based on operational experience, customer insight, and technology that few vendors in this space can match.' This strategy also helped ensure the solution met the company's needs in terms of both operational efficiency and durability."

Success Story No. 2: Nationwide uses real-time analysis to connect with over 50% of its customer base within just 90 days of activity. "With FRISS, 37 months into our relationship, we've now connected the platform with over 50% of our personal auto business transactions and have stopped paying fraud in near real-time!" - Adam Flitton.

Success Story No. 3: GEICO uses AI to affect 30% of the claims decisions. “For causality, Heins said the company deployed the AI to 30 percent of the claims decisions. Employers Holdings, a holding company for several regional insurance companies and one of the 20 largest U.S. workers' compensation insurer groups, is expanding the use of Guidewire’s predictive analytics to manage claims. With the vendor’s 'smart engine' targeting cases expected to involve a very high exposure and 20 percent of the total reserves in the claims.

### 5.2. Impact on Fraud Detection and Prevention

Impact on fraud detection and prevention

Regulators and law enforcement agencies have advised that real-time AI-driven solutions could foster a preventive paradigm in counter-fraud strategies. In particular, the adoption of ML- and AI-driven solutions has witnessed a shift in paradigm in the insurance industry, moving from a traditional 'pay and chase' model to a more anticipatory one, grounded in early fraud identification, rejection, or self-denunciation. Case studies have shown that the deployment of these systems could help reduce fraud losses due to claimant fraud. AI-enabled fraud prevention could cut related losses for an insurance company significantly.

In addition to early fraud detection, real-time AI solutions also aid in ensuring prompt compliance with all insurance-related regulations and policies. AI-enabled insurance fraud detection strategies leverage heterogeneous big data to foster a more efficient and informative decision-making process. The aforementioned elements are considered to underpin the future of the insurance industry and are, therefore, hailed as 'key players' in defining future trends within the counter-fraud and insurtech landscape. The engagement of all internal and external stakeholders is key for the harmonization of the AI solution with the insurer's business model and goals.

## 6. Future Directions

At this point in our survey, an unchangeable fact emerges: we need to cease developing solutions that are capable of detecting features that will constitute the final judgment as a percentage of being a fraud, as we must focus on solutions that can analyze this percentage objectively and change the judgment with real-time feedback. Real-time updates: In the future, it is essential that machines learn continuously to present new

strategies for fraudulent activities, learn to separate and segregate innocent false positives and legitimate frauds without causing harm to the innocent. To some extent, solutions should be developed to combine filtering latent data and, in conjunction with active learning, to mark unusual results on new data treatments. Technological upgrades in advanced technology and cloud computing: Upgraded cloud computing platforms can naturally enhance a system built to handle media data across multiple sources. Illustrations include developments in the ecosystem and machine learning on computing platforms. Blockchain integration and data privacy: In the future, blockchain could be integrated to provide a clear digital asset with no shared data services between companies, government, and individuals. All data is encrypted and owned by the original creator of the data. It is segmented, and the user determines what part of the data will be accessible to users through controlled access smart contracts. Educating insurance professionals: It is highly advisable that technical industry experts get trained continuously in this modern digital world to cope with innovative technologies. Those specialists could possibly help insurance companies understand how to develop new products and aid in slowing fraud. An understanding of these disciplines would help the sector find better insights and reporting tools and might discover potential income loss.

### 6.1. Advancements in AI and Machine Learning

Significant advancements are being made in AI and machine learning that are expected to revolutionize insurance fraud risk assessment in real time. These systems seamlessly process and store information, operate around the clock at high speeds, and effectively detect intimidation tactics in various languages. The development and increase of neural networks have resulted in improved detection accuracy. Neural networks are also being used to detect networks of fraudsters who collude to deceive carriers. Parallel processing techniques have accelerated the ability to search through large datasets for patterns and discover meaningful information.

Sophisticated techniques in natural language processing are enabling machines to partially automate and categorize unstructured text information contained in paper documents. This has the potential to speed operations and reduce the need for some clerical positions, thereby reducing overall costs. Natural language processing can also assist with semi-automated decision-making procedures, thus saving time and

improving the efficiency of claims processing and task automation. The power of today's computers enables extensive and flexible data analysis and predictive modeling, as well as intelligent fraud risk assessment. They can be used to find patterns in data across a variety of sources, recognizing things we don't even know we are looking for. In addition, continuously developing improvements in computers and software indicate it is only a matter of time before we strengthen our capability to enhance real-time decision-making and predictive modeling results.

Continued exploration of this realm promises many enlightening new opportunities, affirming what we already know: it is becoming easier to engage in real time, or even proactive fraud detection. Continuous research in production will shine a light on consumer preferences and emerging coverage innovations. With evolving technology, anything is essentially possible, as long as we welcome new technologies into our innovative fraud prevention efforts. The variety of fields included in this list underscores the importance of staying current with technology trends. It is strongly advised that readers do not close themselves off to new developments in technology and critical thinking.

**6.2. Potential Innovations in Fraud Risk Assessment**

Today's most advanced analytical auditors are capable of detecting various types of systematic and subtle fraud using AI—algorithm topologies such as self-organizing maps, deep neural networks, genetic algorithms, ensembled classifiers, and much more. In this section, we briefly speculate on possible further developments. More sophisticated supervised and unsupervised artificial intelligence, as well as hybrid and probabilistic forms, can help detect more complex fraudulent networks while reducing false positives. Additionally, more use could be made of alternative data sources like telemetry and telematics—ones that are already being collected in the insurance business but are not typically considered by auditors at present. Lastly, more collaboration—real-time or near-real-time—could occur between different insurers and auditing systems, as well as companies that create technology to prevent and detect fraud in the insurance world.

We can envision a time when innovations like real-time individualized pricing and custom contracts, instant claims payments, or new insurance products that intelligently manage risk for consumers become possible. Potentially, the use of instant artificial

intelligence (based on real-time data) can become an industry standard that enables insurers and partnering high-tech companies to easily offer innovative insurance products localized for every state, country, or continent. Importantly, predictions regarding the future of fraud-detecting algorithms require serious ethical considerations. There are definite advantages to detecting ever more fraud. For instance, it could lead to lower premiums for honest consumers. On the other hand, it might raise the issue of what to automate. For example, when insurers detect certain consumer behavior and goals, they may begin to offer alternative insurance products that would limit potential future payouts. Overall, to solve the socially important problem of insurance fraud by embracing new technologies and big data, the industry must think beyond the current technological environment toward possible leaps forward in the future. The insurance industry can be much too insular in its thinking.

**7. Conclusion**

7. CONCLUSION

Efficient fraud management helps to remain competitive in the insurance market. Our research underscores the importance of innovation to keep up with operationally smart fraudsters. Realizing the fraud detection and prevention potential of artificial intelligence in insurance claims, we substantiated action recommendations. The application of real-time analytics, efficient investments, and continuous automatic risk assessment are great promises for the insurance business. Innovations resulting from scientific novel findings are manifold, yet the formulas are one prominent example that are nothing short of necessary instructions for insurance practitioners to implement computer science based on these insights.

Many insurance companies already use AI in claims management and have revealed successful use cases. It has exposed that artificial intelligence technologies can be implemented in very different organizational ways. Compatibility and, in particular, synergy between the innovative technology AI and established insurance company processes are insufficiently understood. Furthermore, predatory innovation is vital to maintaining and developing competitive and efficient anti-fraud technology and the thus implemented AI insurance products, which raise the bar in fraud detection and can serve as a lens for fraudster herd immunity causing all preference to band together. Our work has presented a journey through the state of the art in AI methodologies for the

insurance industry. The research has shown a recent move away from batch data operation towards real-time solutions with the potential to greatly improve the assessment of fraud risk. Surprise value; everyone else is likely still years behind us. In order to keep up with this cutting-edge game, you need continuous access to a lot of case data.