Temporal Sequence Modelling and Anomaly Localisation: A Real-Time Deep Learning Framework for Insurance Claims Fraud Detection

Dr. Christopher Müller, Associate Professor of Human-Computer Interaction, University of Siegen (Germany)

1. Introduction

Today, the insurance companies are facing a significant challenge in the form of detecting fraud in insurance claims. It is projected that approximately 10 percent of all non-healthcare insurance claims are fraudulent, amounting to $40 billion in losses in a year in the United States alone. The prevalence and widespread proliferation of the problem of insurance fraud have elicited the need to strengthen the detection mechanisms to address the issue in real time. This is a critical necessity, especially with the growing sophistication of fraudsters, who present themselves in an aggregated perspective such as organized crime rings. Multiple detection technologies have been explored in the past. However, one of the major impediments for these detection strategies or even the rules-based detection systems in practice is their inability to adapt to and reflect constantly changing risk factors. With the recent advancements in machine learning technologies and the inclusion of AI-driven analytics, it is now possible to have a real-time fraud detection system operational for insurance companies.

Fraud management in general has always been a multidisciplinary concept, drawing insights from the technology space as well as the theories relevant to the process and decision-making, especially in the insurance space. Given the complexity of the issue, the requirement of a laid-back pseudo-process to assure the entities, as well as the burgeoning losses owing to the problem, the insurance process can be considered a unique case in the service industry to approach such fraud detection algorithms. This research entails the task of conceptualizing and calibrating an artificial intelligence-based real-time fraud detection system, specifically designed for insurance claims. The implementation of such a system is promising, especially in the current context when

both businesses and the public are largely relying on technology to manage their claims due to the extended period of lockdowns.

1.1. Background and Significance

Fraud in general, and insurance fraud in particular, has been around for a long time. Professional fraud syndicates have also been established since 1777. There has also been an increase in insurance fraud claims over the years. It has been estimated that approximately 5-10% of all non-health care insurance claims are fraudulent in nature. Insured drivers in Michigan paid an additional $65 per year, primarily due to insurance fraud. Fraud in all lines of the industry amounts to approximately US$ 80 billion annually. The value of all these fraudulent activities is in a range. At present, automobile claims fraud as well as false injury claims have increased nationally. Each dollar invested in medical fraud detection has the potential to avoid or recover $15 in fraudulent claims. If not detected and settled, such fraudulent underwriting, fake claims, and medical claims could cost an insurer a lot of money, time, and trust with policyholders. In addition to financial losses, a single fraud could also have positive effects. The destructive impact such circumstances may have on the effectiveness of insurance systems renders insurance immeasurable for unfortunate and unlucky persons who use it honestly. In an environment where premiums and tax policies are becoming increasingly unaffordable for many residents, combating fraud is increasingly important. Furthermore, if organizations are unable to properly resolve fraud, their image, including market and distribution, will suffer. There has also been revolutionary progress towards artificial intelligence, which has the potential to identify and combat insurance fraud. Knowledge of incidents and claims is needed in order to be able to combat insurance fraud in real time. However, it was discovered that unreliable information syndrome is caused by various biases, lack of historical reports, and the time it takes to be reported, authenticated, and audited. Humanity and technological developments as well as new discoveries are bringing about improvements in human life. At first glance, historical insurance fraud data might seem to be unrelated to technological advancements. This view is not appropriate, because there is a relationship between them. Rather, frauds are classified according to a mixture of fraud techniques. This research is therefore significant, as it uncovers these fraud patterns based on years of medical fraud data. A useful hallmark of fraudulent financial transactions falls into this category. A thorough review was conducted on intelligent agent-oriented systems

and on the related topics. This chapter was sometimes referenced as a foundation for the principles that could be utilized for the computer-based attack analysis agents.

1.2. Research Objectives

This study aims to identify current algorithms and techniques used in fraud detection to predict and identify fraudulent insurance claims based on a research review. The primary purpose is to improve the accurate detection of these claims utilizing machine learning algorithms in real time to prevent the approval of fraudulent claims. This is intended to provide the capabilities for organizations to validate potentially fraudulent claims before their approval for payment, resulting in increased success and reduced aftermath of any later charges made. The current emphasis of fraud detection in the insurance industry focuses mainly on offline detection, primarily utilizing descriptive statistics interpreting textual data from prior detected fraudulent claims. Thus, they may have low real-world accuracy. Therefore, one focus of our objective will be to test future real-world scenarios in utilizing such AI applications to improve fraud detection rates. This study is intended to produce a comprehensive, effective, and efficient AI framework for the real-time assessment of insurance claims. The analysis will assess the current scientific knowledge and processes using data from 28,000 false and legitimate insurance claims between July 1, 2016, and January 15, 2017. In order to assess these, two main objectives have been identified. The first is to determine the current algorithms and process techniques used in AI-based applications for insurance fraud detection based on scientific literature. A second, and the most relevant objective, is to determine the relative efficacy of the major AI techniques to predict and compare application capabilities used in real-world testing for the detection of fraudulent insurance claims in real time. These results are to be used as a foundation for future AI models, making maximal use of AI value to the organizations in the insurance industry by fusing them into the real-time detection processes they are currently practicing. In this way, the AIs will primarily focus the process on assisting the human detection workforce, thus avoiding the so-called backlash problem.

1.3. Scope and Limitations

The goal of this paper is to design and curate data pipelines for subsequent computational models that can extract structured information from insurance fraud databases in Norway, focusing on fraudulent medical expense claims and life insurance

claims. Available information in unstructured medical fraud data will be used to inform and restrict the extent of insurance claims to be used in the subsequent computational modeling. The goal of these models is to predict fraud in insurance claims. We will focus especially on deep learning networks and their advantages and disadvantages in the communication of trust in explanations for predictions. We will further elaborate on interpretability and present metrics measuring trust. In this study, we limit our scope to insurances within the geographical territory of Norway. The study has its focus on medical expense claims to the Norwegian Health Economics Administration. The study further includes life insurance claims to the main Norwegian life insurer. We limit the scope to insurance claims from the year 2019, as it currently has the most recent complete data available. We will examine a variety of methods and algorithms, and we will be looking at both machine learning and computational models. We will focus on, but not restrict the analysis to, the application of real-time AI-based analytical methods. There are several limitations to this study. First, the information used for the study is restricted by the data that are available. Data restrictions include, but are not limited to, lack of geographical distribution in life insurance data, lack of information in the permanent invalidity claims, and defined age spans of the data. Some fraud cases may have been missed or gone through the nets in this setup. Moreover, since not all companies have submitted fraud cases, we do not have a complete overview of all detected fraud claims in the actual insurance databases. Data can be very noisy and thus the extracted structured data for the analysis are human decisions and subjective. Our choice of analysis methodologies can also have weaknesses and limitations, and implementation could therefore affect the results. Some predictors may have more correlated factors than other predictors due to more complex research theory, and this can present a biased view.

2. Understanding Insurance Fraud

Insurance fraud is any act committed with the intent of wrongfully obtaining a benefit from an insurer. The fraudulent activities may involve individuals closely associated with policyholders, the policyholders themselves, professionals involved in the insurance claims process, or organized rings of claimants primarily aimed at obtaining large payoffs. The list of fraud schemes is diverse, including feigned accidents and hospital visits, counterfeit pleasure craft thefts, and catastrophe-related insurance fraud such as fraud after natural disaster claims. Insurance fraud not only impacts the

revenues and profits of insurance companies but also the resulting economic effects of increased premiums and reduced coverage for policyholders. The consequences for the individuals perpetrating the fraud are significant as well, including the potentially severe legal ramifications associated with fraudulent activities that involve many insurance claims.

Fraud may be classified as either hard or soft. Hard fraud includes staged accidents, arsons, and workers' compensation fraud in which nonexistent or previously sustained injuries are used as the basis for false claims. Hard fraud claims are reportedly more difficult to detect as they do not fit typical loss patterns. Soft fraud includes evidence of manipulated claims that exceed the insured incident's actual value, such as staged accidents. In addition, many fraud types can be segmented via either a special niche such as auto insurance fraud or bank fraud, or specific claim types such as a surreptitious staging of workplace accidents or padding home claims with unrelated property theft, vandalism, or weather-related damage. Some fraudulent behavior patterns are permanent, such as those disfigured in accidents; others are temporary in nature, such as those pretending to need assistance navigating into vehicles after an accident when not observed.

2.1. Types of Insurance Fraud

Medical Claims Fraud

- This type of fraud is related to health insurance policies. The Department of Justice and Health and Human Services spends each year to investigate health care fraud in the United States. Perpetrators of health insurance fraud can be groups of fraudsters who work together or individuals. Many times, these fraudsters are patients working with the fraudsters and making money while obtaining health care services needed. False claims include Medicare, Medicaid, and private health insurance programs that are often vulnerable to fraud.

Auto Insurance Fraud

- Auto insurance scams are the most commonly spotted type. One in ten people makes false statements. Approximately is lost from insurance scams. This type of scam is run in a variety of ways, such as staging fraudulent accidents, inflating fees for surgeries and

other medical treatments, claiming additional care, intentionally damaging the hood of the car, and much more.

Property Fraud

- Types of property fraud are rare, but they exist. The perpetrator initiates a scam charge after a property claim occurs. This usually happens when the asset's value is more than what might be fixable.

Workers' Compensation Scam

- Workers' compensation helps employees compensate for an injury or illness they sustained in the workplace, providing temporary disability benefits or even lifelong benefits. Some people who cheat the system may fake injuries to collect money, even if they are either recovered or not hurt at all, or work underground for extra cash. Some examples of scams in workers' compensation include fictitious injuries and misclassification of employees.

2.2. Common Techniques Used in Insurance Fraud

2.2. Common Techniques Used in Insurance Fraud

The insurance industry is a multi-trillion-dollar industry and is not without its share of fraudulent activities. Many techniques are used by individuals, singly or in groups, to defraud insurance agencies. The less sophisticated techniques employed are commonly manipulative in nature, such as padding bills, faking car accidents, staging car crashes, and selling non-existent policies, while the more sophisticated attacks that are carried out use the system itself to defraud agencies.

The man-made accidents and office-based deceit are often what comes to mind when one thinks of insurance fraud. However, quite a few modern channels of tricking systems, including those that use technology: fraudulent web pages, electronic signatures, cross-border insurance fraud, and online sales; involving fraudulent web page drives, infecting systems to cause damage or data leaks, and falsification of online social media as susceptible areas for attack. The recurring theme is essentially one that suggests current research is misled by traditional approaches and thoughts about insurance fraud. This implies that not understanding the necessary skill set possessed by newer fraudsters and trusting in tradition may be behind the decrease in the

performance of fraud detection systems. The solution is the incorporation of reactive, analytical systems.

Typically, available business intelligence tools provide business managers with insights on their data. Two types of experience can be recorded in such systems: (1) being first to discover potentially fraudulent activity and (2) returning a fraud case as part of a dynamic learning strategy. The first provides support for business developers and managers by providing timely and 'on-the-spot' information. However, this information is dependent on the experience of the individual; whereas the second type of experience identified provides a second tier of alert to continue safeguarding the profit margins and to ensure fraudsters are unable to alter their actions. This level may result in large reaction levels but is justified because the threat is greater. Such information would be directed at the business policy, with insurers using the information not for rejection but for policy. Different policies will produce different primary results as to the kind of fraud detected. The corollary to the dynamic policy design, real-time analytics Dynamic Fraud Detection technology is therefore preferable because it will be able to change the regime of a trusted operator in order to generate false positives. For this to work, the system must be employed continuously lest fraud is not detected as quickly as the fraudster adapts.

3. AI and Machine Learning in Fraud Detection

Artificial intelligence and machine learning are revolutionary in the field of fraud detection and are thought to be the transformative force of the insurance sector. AI is a theory of human intelligence that includes machine intelligent processing. Machine learning is a kind of AI whose nature is statistical learning - learning from available data input and data processing to make a decision. Although traditional statistical methods can reach about 95% detection accuracy, they can't compete with new methods in terms of speed. Given that, traditional methods need to investigate large data sets and therefore take more time to achieve results, while AI can cope with this work faster. Supervised learning algorithms are very popular for fraud detection since labeled data is always available. Every record is labeled as either fraud or normal. Some common algorithms are decision trees, logistic regression, support vector machines, and neural networks, each of which has different features. Unsupervised learning is the other type of solution, used when there is not a sufficient amount of labeled data and when the

software needs to discover patterns. Some well-known algorithms are K-Means, hierarchical clustering, and DBSCAN clustering. Semi-supervised learning is the third type of artificial intelligence algorithm used for fraud detection, where human beings provide a small amount of classified and unclassified data, and reward systems classify in a controlled environment, ensuring high performance. It is also possible to use wide learning, combining positive training specimens with thousands of unclassified cases to recognize new types of fraudulent activities.

3.1. Overview of AI and Machine Learning

Artificial intelligence has witnessed rapid advancement in the past few decades. Subfields of machine learning can be classified into broad taxonomies based on the learning task being performed on the data. These include supervised learning (where a model is trained on labeled data), unsupervised learning (where a model is trained on unlabeled data), semi-supervised learning, and reinforcement learning. AI research is founded on the availability and collection of large, diverse datasets. A significant leap in the capabilities of machine learning models in many domains occurred as a result of the availability of large annotated datasets. Advanced algorithms combined with extraordinary processing power have made it possible to search across large sets of data in real time, making the use of AI an increasingly tempting choice to detect fraud in the insurance domain.

Recent advances in AI technologies have boosted real-time processing capabilities on big data. Optimizations of existing algorithms and the invention of newer, faster models now allow us to train, tune, and assess models on that massive quantity of data in near real time. Numerous algorithms are now available that facilitate quick, realistic results, for example, stochastic gradient boosting, AdaBoost, neural networks, Naive Bayes, and others, to be used in some combinations and sequences for data processing. Many of the algorithm advancements, such as those happening in neural networks, unsupervised learning models, and reinforcement learning, while highly exciting and offering theoretically groundbreaking opportunities, are currently underutilized in insurance fraud detection or have not yet reached the stage to compete with or supplement current algorithms.

Algorithmic selection is a key guiding principle toward effective data mining and subsequently fraud detection. The selection and choice of which algorithm to apply is

critical, as different algorithms focus on different types of relationships between data constituents. This determines the accuracy of the model and can accordingly lead to potential hurdles or rewards in terms of operational costs to monitor and review false positives in a real operational environment. Best practice algorithm selection will enhance the efficiency and effectiveness of detecting fraud. Also, in detriment to AI uptake, bias in data is one of the main concerns looming over AI adoption. The lack of interpretability of models can have dire consequences, particularly in insurance fraud scenarios. The current models are developed using statistical tools that are completely transparent. A model based on artificial neural networks would not only be a "black box," rendering it unviable to encourage compliance with the best behavioral choices and activities that preempt insurance fraud.

3.2. Applications in Fraud Detection

At its root, AI and machine learning allow algorithms to process data, identify patterns of normality, learn, and on a continuous basis adjust a standard of comparison for the recognition of unusual patterns. Machine learning systems, through their ability to connect to and analyze vast historical datasets derived from diverse sources, provide a higher predictive capability than traditional statistical models and have the potential to bring business processes to a new level regarding real-time assessment. A behavioral monitoring tool agnostic to numerical or image input has the same application domain as the claim-based fraud scoring algorithm, with use cases and challenges that are very similar. This could be applied to a wide range of different domains such as churn prediction, claim fraud detection in the motor industry, premium evasion in health insurance, credit scoring, voting on the go, and sports match outcome predictions. However, a typical example of an area that is greatly benefiting from the application of the technology in live assessment is fraud detection, both in claim fund systems and in superannuation systems. The survey indicates that fraud and its detection are becoming an increasing concern. It shows significant trends. An overwhelming percentage are focusing on predictive systems for fraud detection; a large percentage are concentrating on real-time detection as a priority; and a significant percentage rely heavily on developing stronger relationships with and between enterprise staff to help detect and prevent fraud from occurring. The survey demonstrates a trend that we are experiencing with customers - a move away from "passive" mechanisms to "active" detection. Having potentially identified a fraud, it is critical to take legislative requirements into account.

Strict privacy and trade practice laws, personal account information handling at both state and national levels, require compliance with policies that must be enforced to avoid fines. Currently, if an organization does not check current and historical relationships when investigating a fraud case, they risk various fines, with fine amounts increasing significantly for privacy contraventions. Additionally, a large government entity currently utilizes a system in a privacy review capacity. This system is used to check that the monies it is paying out are to the correct people, for the correct amount, at the correct time, ultimately preventing privacy contraventions.

4. Data Collection and Preprocessing

Insurance companies collect and compile data, some of which is highly sensitive about both the policyholders and their insurance claims history. The collection of the relevant data is an important issue. Many different sources of data for risk assessment and fraud detection are available and could be used. An improved or more complete dataset may therefore be available or achievable. Whatever the source of the data, an inference may be made from model-generated variables; again, a model implies a simplification of the world from the true underlying mechanism. Besides the absolute value of a variable predicted or captured by a model, the impact of that variable is relevant to fraud detection. Common before frontline models are running, the underwriting models probably make or provide separately the predicted or captured value that is less open to manipulation or hardening, required as input for a fraud detection prioritization model.

In this manuscript, very limited detail is given on the way policies are rated and hence claims are estimated. The next relevant issue is to train the models, thus the training dataset used. It is the measurement of fairness in three models that needs a separate discussion. Based on the data sources integrated and the subsequent matching of the vehicle's make and model, four distinct datasets become available. The definition of the input variables is used to illustrate the process. To invoke the models, this set of predictors is chosen. The boundary is estimated in a straightforward manner by asking for the desired number of records. Keep in mind that a smaller sample size would create an imbalance between the observations of the base case and those of the suspect.

4.1. Sources of Data

When considering the nature of data needed for an AI-enabled fraud detection system, one basic distinction can be made regarding the data's structure. Structured, semi-

structured, and unstructured data can be differentiated. Internal data is an example of structured data. This includes historical information on policyholders and their claims, as well as explicitly declared information by the insurance company and records of agents' activities. This type of data is usually complete and clean. Examples of internal semi-structured or complex data include telematics or sensors. External data is, more often than not, independent of the insurance company.

Besides the data sources concerning relevant actors, like policyholders or third parties, there are psychological factors to consider. Clients, including third parties, may have similar concerns, particularly concerning privacy. Because of the need for data from various sources to establish comprehensive analysis, the size of the fraud ring and, therefore, the number of data sources needed increases. Some of the initial empirical cases using multiple data sources for fraud detection were presented. Data sources of different levels should be harmonized and integrated. Yet, integrating data from different sources is not easy because of differences in processing and storage systems, deployment settings, and privacy and policy constraints affecting data integration. For example, data confidentiality measures may prevent the sharing of data between banks, insurance companies, and the police. Furthermore, when integrating data from different sources, the consistency of the integrated data must be ensured.

4.2. Data Cleaning and Transformation

The next step after obtaining the insurance data is to clean and transform the dataset into a deployable form that can be used to run different machine learning models. Data cleaning plays a crucial role in the process of data analysis. Good-quality data ensures that analysis results are reliable and accurate. A data scientist must pay attention to the problem of inaccurate, inconsistent, or low-quality datasets. One common problem is the issue of duplicated entries, which can lead to the exclusion of those field records, rows, or columns. Another quality problem is inaccuracy. It is the procedure to cross-verify your entity, attribute, and relation with the real world. Remember, the role of feature engineering is to transform raw data into a format that can be used by classifiers to build models. Each stage in the process of cleaning the quality and pandemic data may perform some submission tasks. After the ETL process, data transformation is done. Transformation steps ensure the dataset has the necessary input for the model application. This includes normalization, encoding, grouping, and outlier detection and

can involve missing data handling sessions. Clean data is used to convert raw data into a format that is easily used by the model. For example, categorical values are generally translated into numerical ones by encoding.

Data transformation is a crucial step before the model can be used by the data analyst in the dataset. One way to transform data is through data dictionary processing. This is primarily done by categorizing, encoding, normalizing, and handling missing values in the dataset. The process of cleaning and transforming data involves understanding domain knowledge about the data. As a data cleaning practitioner, one must possess good domain knowledge to be able to convert certain data into its real form. Poor quality data leads to poor model results. Unsustainable models cannot be utilized in developing machine learning. Modeling is not the only final step in the categorical base of the features learning process. Fortuitously, the usual limitation in most instances of this method is that the origin of bad results is bad quality data. A well-thought-out cleaning process, and the willingness to accept that models cannot be constructed due to weak data quality, is more important in many locations. Data cleaning and transformation are critically essential when implementing machine learning or AI applications. Quality data is the foundation of fraud detection in insurance claim processes using AI.

5. Building and Evaluating Machine Learning Models

Model Selection

Choosing the right algorithm for a machine learning model depends on various properties of the data at hand. Therefore, the datasets should be carefully analyzed to choose the suitable algorithm. Evaluation metrics are needed to measure the model's success; some of these metrics include:

1. Accuracy, which measures the number of correct predictions made as a ratio of all predictions. 2. Precision, which calculates the ratio of correctly predicted positive observations to the total predicted positives. 3. Recall (sensitivity), which is the ratio of correctly predicted positive observations to all actual positives. 4. F1 score, which measures the model's accuracy more completely than the other metrics.

Cross-validation is a vital step performed during the evaluation of the model. It assists with determining the accuracy of empirical results and is greatly supportive when it

comes to assessing the model's generality. Feature engineering, the extraction or transformation of features to allow the machine learning algorithm to actually learn, is an essential stage in the development of machine learning models.

Engineered features usually tend to improve the learning model, providing additional knowledge about data through domain experience and giving a chance to validate the model with created features.

Model Training

After the preprocessing of the data, the model can be trained and tested. The model's training process refers to the gradual escalation of its predictive strength as adjustments are made to parameters. To evaluate the performance of the model in a more effective and productive manner, various approaches can be used to validate the efficacy of the model. The model's accuracy is validated and found to be reliable throughout the creation and verification of results. The process of creating a machine learning model is often shown to be iterative, as there can be stages at which the model needs to be revisited to achieve the most promising results.

5.1. Model Selection and Evaluation Metrics

Although there is no universally accepted algorithm that can be best used for fraud detection, the choice of the algorithm may depend on the criterion set by top management. Some managers want to understand the reasons behind the system's prediction, so they are more likely to choose algorithms that can be interpreted, such as decision trees, at the expense of sacrificing accuracy. Others are more interested in computational efficiency and accuracy rather than interpretability. Several algorithms have proved to be reliable and sufficiently accurate for fraud detection, such as K-Nearest Neighbors, Decision Trees, Random Forest, AdaBoost, XGBoost, Neural Networks, and Naive Bayes. However, decision trees and their derivative algorithms, such as Random Forest or XGBoost, could be solid interpretative algorithms for fraud detection that often yield the best results with other algorithms under many circumstances. Numerous possible dimension reduction techniques and feature selection methods, as well as ensemble methods, could improve the capabilities of the used algorithm to identify fraudulent cases. An additive tree-based model, an extension of

decision trees as well as Random Forest, based on real field data in automotive insurance, is used as a service for risk officers.

Based on the same benchmark data set as an example, a plethora of evaluation metrics, such as confusion matrix metrics and threshold-independent metrics, could be generated and studied. Proper selection of one or more evaluation metrics, depending on needs and trade-offs between them in operation and decision-making, is vital for conducting research and facilitating the field of fraud detection, particularly for the implementation of fraud detection systems. For example, if minimizing the false negative rate would lead to reckless claim investigations to the detriment of the entire operation, higher value should be placed on specificity and minimizing the fraction of non-fraudulent claims incorrectly identified as fraudulent. Similarly, a high false discovery rate translates into operational costs for the number of flagged claims that need to be investigated manually; therefore, it would be considered a significant performance measure. Numerous metrics could illustrate how one solution is better than others and must be selected as they balance trade-offs between two groups of decision-making and operation by a business partner if a choice has to be made regarding different competing systems or algorithms. For example, a perfect predictive model against mortgage fraud, unemployment fraud, or sick leave fraud might not be of interest if the rule based on such a model implies no mortgage, allowance, or sick leave has ever to be given. Therefore, a balance between preventive and detective costs has to be sought. However, building a classifier for which all performances are high for any class is difficult, if not impossible. Finding an optimal classifier is always a learning and design process.

For fraud detection and banking credit scoring in general, two types of costs are involved. The first one is the cost of a harmful application not being identified, which represents the loss rate associated with some predictive rules. This loss will be represented by the fraction of frauds that are not identified in the case of fraud. High enough loss rates could result in such applications being deemed non-acceptable. In such a frame, it would be crucial to maximize the correct identification of non-approved applications (i.e., the number of structured non-fraud cases that are correctly differentiated from the fraud cases). This might be addressed by the usage of specific

ROC curves since the curves illustrate the trade-offs between the false positive rate and the true positive rate.

5.2. Feature Engineering

Once the model has all the necessary features, these must be selected and engineered to make the pattern of fraud detection evident to the model. It is also very important to have domain knowledge when it comes to selecting the most relevant features in this regard. We selected the ten benchmark datasets for which we selected the most relevant features. The creation of new features from the raw data can be approached in different ways. It requires domain knowledge regarding the problem at hand and the operation of the company. Feature selection and feature creation are critical. These features will be used as inputs to our models to forecast fraud.

- The creation of an alert for a longer period before approving a claim: use the difference between the date of the claim and its approval as new data, which has proven to be significant, since a longer interval could indicate that there are more exceptions and therefore an increase in the probability of fraud occurring. - Engineered feature for nominal attributes: there are techniques that make it possible to achieve the transformation of nominal data into quantifiable data without categorizing them. - Scaling: it is the process of aligning and standardizing the attributes of a dataset. It must be done because the different variables do not have the same ranges and the same units. - Some features might not be relevant or might have a high correlation to one another, and this situation, called multicollinearity, can cause instability in the model. To speed up the computations, the decision can be taken to discard these features and select the features that have the biggest influence in detecting fraud, depending on the domain, since in insurance fraud detection, some of these features usually have more weight than others. - Techniques like Principal Component Analysis have been used for both operations.

5.3. Model Training and Testing

Training machine learning models for the purpose of fraud detection is similar to training models for other tasks. To avoid overfitting, it is common to split the data into three hold-out sets: one for training, one for validation, and one for testing. The iterative process of training, validation, and model adjustment is repeated until the model's

performance plateaus, or stop criteria are met. During this iterative process, the model's architecture should also be substantially altered to avoid small steps in local minima.

The simplest method to evaluate the performance of a trained model is through dedicated test sets. Metrics such as accuracy, precision, recall, and F1 score are standard performance measures, which have direct interpretations for fraud detection. However, a trained machine learning model will perform differently on the test set than in a real-life production scenario. In order to measure the real effectiveness of the model, it is important to compare a test with and without the model in a real-world setting. This is typically done through tests. To avoid drastically slowing down training by using the full dataset, the model is typically trained for a number of epochs using a smaller sample size. After it is determined that the model's performance plateaus, the model is trained until it has seen the entire dataset the number of times dictated by the configuration.

6. Case Studies and Practical Applications

While a great deal of activity in recent years has been focused on the development of AI-based support tools for the detection of insurance fraud, it is also important to remember that the ultimate measure of an AI-based detection tool, or indeed any fraud detection system, rests on its practical application. In this section, we present a number of real-world case studies that afford a glimpse into the practical application of AI-based fraud detection in the insurance industry. Given that the true value of an AI-empowered fraud detection tool or solution is to a large extent realized through the successful execution of strategies in detected cases and through the insights gained from feedback loops, the successful application of AI in practice sheds light on these aspects.

The case studies presented in this section show that there has been a growing interest across the insurance industry in deploying AI-facilitated fraud detection systems during the last few years and that there have been some notable successes in this regard. Each of the implementations outlined in this section is discussed in terms of the different AI techniques used and the challenges encountered and resolved through the deployment of these technologies. Throughout, the case studies highlight the many lessons learned from real-world deployments, as well as addressing the potential improvements to the systems and techniques under study. The purpose of including these studies here is to provide a clear link between the disciplines of AI and fraud detection. Furthermore,

these studies serve to illustrate that the fraud detection strategies presented in this report are more than pure theory.

6.1. Real-World Examples

Levenaviv, one of the largest insurance companies in Israel, is leveraging predictive analytics. As part of an interdisciplinary process, multiple teams must assess and evaluate risk. Levenaviv has implemented a fraud detection model as one such technique. The model took into account a variety of factors including claim size, corporate reputation, claim validity, the accident's circumstances, chronological data, and general information on the car and its driver. The analysis revealed that, although working different overtime hours, both automobile claims and claims of the art segment often got caught. Insurance companies were able to use this system to save dozens of NIS of insured capital. Another large insurance company has also begun implementing serious measures to detect fraudulent processes. A major insurance company plans to adopt a similar strategy as a way of examining more claims.

One insurance company offers online claim settlement, no independent opinions, and standard claims controls. Their company has also implemented advanced claim processing systems to find out in real time whether the claimant really used the event. Consulting companies have stated that the company is aiming to implement artificial intelligence technologies that aid in the detection of anomalies and patterns used to forge documentation and identify the likelihood of fraud. These can include facial recognition, geolocation services, chatbots, drones, and social network reviews. It is possible to schedule a physical survey on an exceptional basis. The profit of a policy is increased because of human costs but also because people are honest. Despite the main advantages of an automated claim control system, some limitations must be taken into account. Analysts are concerned that generating too many false positives could lead to a loss in profit; if field inspections are carried out, they could damage the company's reputation. The company also made a small investment in a startup company to test intuitive devices collectively in neo-experience insurance. The startup will be able to offer direct insurance cover for drones. The current theory has already led to actual technological implementations and further emphasizes the importance of continued innovation.

6.2. Challenges and Solutions

Challenges and Solutions

Most of the challenges during the implementation of AI-based systems for fraud detection are not specific to the insurance sector and are largely pervasive. We discuss the challenges based on their impact on the effectiveness of fraud prevention, detection, and response, as well as personal data protection.

Data Privacy

The handling of personal data in AI systems raises novel questions related to data protection, transparency, and accountability. The introduction of the "right to plausible explanation" allows consumers to obtain the most precise information for why their application might have been denied in order to have a possibility to appeal the decision.

Compliance

The correct interpretation of legal ambiguities when applying AI systems for fraud detection in insurance is a major challenge. Several new models have recently been proposed for creating insurance contracts based on data provenance and trust management.

IT and Technical Integration

In contrast to internet search and advertisement markets, the insurance sector is significantly more fragmented, and many businesses, especially in the reinsurance sector, are based on B2B contracts. Consequently, insurers have strong motivations to invest in data science, machine learning, and AI while keeping information hidden from competitors or potential adversaries.

The existing barriers for potential data sharing tend to prevent the development of sound strategies in AI fraud detection. We argue that the establishment of best practices and guidelines for fraud detection in insurance could foster knowledge and data sharing. Think tanks or working groups designed to minimize risks between different stakeholders could therefore provide efficient communication channels and foster innovation in the area. Malware techniques are likely to become more polymorphic and unpredictable. The tuning of AI models should therefore not be use-case specific but

rather focus on creating the most general AI algorithm that revises itself over time through continuous training and retraining to prevent any serious unexpected vulnerabilities that are not simulated in advance.

7. Conclusion and Future Directions

This study aimed to research the capability of artificial intelligence in detecting insurance claims fraud in real time. Although there have been significant advancements in the real-time forecast of various healthcare populations and securities, there exists scarcely any real-time fraud detection system in insurance. From the study, we conclude that an ensemble of state-of-the-art learning systems, that is, machine learning techniques and deep learning frameworks, can offer a better principal framework, which is significantly able to decide if the case of an insurance claim is fraudulent. This research successfully accomplished the research objectives covered in policies, data and preprocessing, model analysis, and results sections. The conclusion of this paper incorporates the significant achievements drawn from discussions about these sections. This research is potentially revealing to companies and industry by significantly enhancing the manual efficiency of fraud detection in conventional techniques.

AI-based detectors in real time have the potential to revolutionize the ability to combat insurance fraud. As such, emerging AI technologies should be continually checked and agents trained as to their use and importance encouraged. Various legal, regulatory issues, and ethical considerations also warrant further research. AI and related technologies in a more non-economic light may place limits by linking people or groups to insurance products if they are not careful, breach regulatory and ethical requirements, or possibly offend existing regulations. It is also worth mentioning the need for additional research in developing machine learning-based algorithms, in view of the possibility that such developments will drive us to work on a deeper understanding of data and of how we can consider the design, instead of working excessively on the technological side.

7.1. Summary of Findings

In this research, we examined how technologies, especially artificial intelligence, contribute to fraud detection in the insurance industry, with a specific focus on insurance claim processing. The emphasis was on AI because learning algorithms are improving year by year due to increasing computing power and the availability of data.

Therefore, machine learning algorithms, which fall into the field of artificial intelligence, were seen as a valuable addition used to enhance the detection of fraud in insurance claim scenarios. For the insurance industry to fully take advantage of new AI technologies, the following steps related to data collection, model implementation, and model evaluation are needed. Skipping one of the steps can lead to inefficient models that are unable to distinguish good customers from bad customers. Throughout the main body of the report, seven case studies were conducted that revealed many similarities and differences between the insurance companies. It is worth noting that the tactics of fraudsters and the types of fraud are constantly changing; they evolve beyond existing methodologies. Therefore, it is of vital importance for the insurance industry and its partners to further develop software systems to detect fraudulent claims accurately. The main and final conclusion from the report is about the realization of early detection of auto claims fraud, and especially, knowledge of the latest fraud in the industry. It is also critical in the development of accurate insurance risk selection for better underwriting. Overall, data management and AI play a very strong role in fraud detection. Fraud detection in the insurance industry cannot be separated from data accuracy and AI. The objective of the group is to design a case study and provide a deep analysis of fraudulent claims and the potential for developing a system that can assist in the early detection of fraudulent claims.

7.2. Implications for the Insurance Industry

Implications for the Insurance Industry

The findings have far-reaching implications for the insurance industry. By focusing on real-time AI-based fraud detection, this study indicates the potential of state-of-the-art technologies to transform existing methods of detecting potentially fraudulent claims. Currently, insurance contracts contain fraud and fraudulent behavior monitoring clauses; integrating strikingly accurate real-time AI systems into the monitoring process would not only free up resources in the claims department and drive down the operations budget but also create opportunities for larger-scale fraud detection in daily business. When operating on these larger data sets, insights that previously could only be claimed by business analysts after several months of systematic investigation or econometric modeling become readily available across the company – opening up genuine possibilities for retaining existing customers and attracting new ones. This is

operationally very different from the feel-good strategy where pointing in the general direction of AI-based evidence can help along sales processes without delivering real strategic industry insights. Our contribution is the pragmatic integration of AI research output into an existing service offering to expose its proof of value in a real industry context.

Today, real-time decision competencies based on factual data have direct operational value in the short term, offering protection from speculative financial success of start-up tech firms. 'Playing it safe' while merely increasing budgets can, on the contrary, lead to insurance firms falling behind. The numerous case studies we have conducted with claims management departments indicate the conservative nature of the industry – with good reason. Very few tech offerings on paper will present an industry with a long-term edge; hence there is little impetus for our incumbents to invest without operational evidence. By providing this study with a scientifically sound empirical basis and proof of concept for the 5-year period from 2015 onwards, we give a vision of exponential growth in this field. More is to be done regarding the long-term potential should the insurance firm be willing to open their data, but if such results hold, the timeframe for moving to stage two would be around 2025, further adding to the limited short-term risk of investing in the present, more limited explorative study. Operatively, insurance firms stand to achieve immediate evidence regarding expansion feasibility in markets other than the UK, with a focus on Europe, as this is the geographic region that does not just share true data with the UK insurance branch but also where significant assets of interest to an Australian company are held. Through this strategy, firms would have direct evidence to support a shift in what is typically 'benchmark fraud' rates in Europe and come to dominate large segments of the Austrian market through data-driven strategic innovation.

7.3. Future Research Directions

The in-depth investigation of possible root causes for these low confidence values was not in the scope of this and the current preceding study. Future research should explore these root causes and artifacts, as well as ways into relevant practices for insurers and insurtechs. From the findings in this and the preceding study, implications for a number of further research directions can be derived: The potential impacts of emerging and developing technologies on the employed strategies for fraud detection should be

further studied. Future work could extensively explore the possibilities for combining blockchain and AI-based image recognition systems for saving and using claims photographs in a highly secure, verifiable, and usability-enhanced way.

Research should further elaborate on the added values of AI-based fraud detection for an insurance company's processes and offerings, including its business models, business model elements, and relationships with its customers which are based on trust due to potential positive impacts on customer acceptance and satisfaction. A thorough exploration of new collaborations between academic and practice-oriented researchers from the fields of business administration, computer science, and mathematics, as well as insurance companies and policy practitioners could bring valuable insights into the intertwinement between technological, business theoretical, and practical aspects of AI-based fraud detection in insurance claims. Due to the fact that both this and the preceding work relied on technical measures in order to identify unknown fraud cases and these measures were fed with historical values to first build the necessary models, it is essential to innovate methodological approaches for checking data based on legal and ethical considerations for data use and privacy. Significant endeavors should be made in this regard, on the one hand for innovating large-scale investigations of policyholders applied by way of immediate action in the case of reasonable doubts about the accuracy and sincerity of the policyholder interviews, and on the other hand with a closer look at trust issues in the application of methods for emotion recognition and data verification purposes in claims settlement processes.