AUGUST 30, 2018

HEALTHCARE: FRAUD DETECTION

YDI SOLUTIONS

Presentation Rundown

Points of Discussion

Introduction
Types of Frauds
Frauds that can be detected by AI
Proof of Concept
Conclusion
Contact Us

Introduction

Insurance fraud is an illegal act on the part of either the buyer or seller of an insurance contract. Insurance fraud from the issuer (seller) includes selling policies from non-existent companies, failing to submit premiums and churning policies to create more commissions. Buyer fraud can include exaggerated claims, falsified medical history, post-dated policies, viatical fraud, faked death or kidnapping, and murder.

Insurance fraud is an attempt to exploit an insurance contract. Insurance is meant to protect against risks, not to serve as a vehicle to enrich the insured. Although insurance fraud by the policy issuer does occur, the majority of cases have to do with the policyholder attempting to receive more money by exaggerating a claim. More sensational instances, such as faking one's death or committing murder for the insurance money, are comparatively rare.

Most common schemes which are exploited in insurance fraud include: Premium Diversion, Fee Churning, Asset Diversion, and Workers Compensation Fraud.

Types of Frauds

Most common types

Deliberate and Opportunity Fraud –
Deliberate fraud is purposeful act of presenting accident or loss which is covered under the policy. Whereas, opportunity fraud is created by a policyholders by over stressing a genuine claim or providing wrong information related to the pre-existing diseases etc. to get the underwriting done in their favor.

External and Internal Fraud –
External fraud is claimed by either an individual or entities like policyholder, beneficiaries, medical service providers or vendors against a company. Internal fraud on the other hand is carried out against a policyholder or its company by other employees like manager, executive or agents.

Policyholder's Fraud –
Now-a-days, consumers have become aware of the norms, features and rules of the insurance and have started getting benefited by being involved in frauds. Policyholder frauds are divided into 3 categories – eligibility fraud, claim fraud and application fraud.

Types of Fraud

Most common types

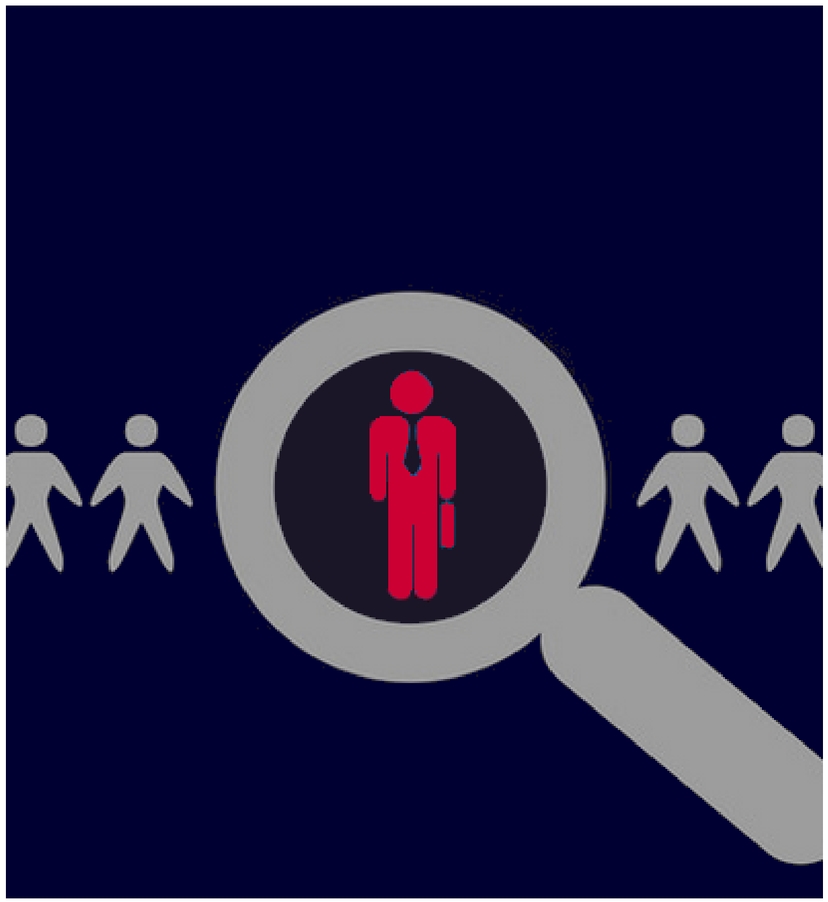
Eligibility Fraud -
This fraud generally constitutes the falsification of the information provided about the insured's employment status, pre-existing diseases or information concerning the dependent. Here, the beneficiary is paid benefits illicitly, for example, if a person submits claim for the dependent or relative who is not covered under the policy.

Application Fraud -
The consumer knowingly enters forged information in its application related to the pre-existing diseases, claim or important dates. A policyholder might not enter the details related to his pre-existing diseases or serious medical conditions in order to get an extensive cover and have problem free claim filing.

Claim Fraud –
When a consumer enters an illegal claim for whose benefit he is not entitled for, the fraud is called claim fraud. In such intentional cases, the provider and member are seen to go for collusion and thus, benefiting the physician. These kinds of groups are also known as fraud rings.

Frauds that can be Detected by AI

Cutting Edge Technology Method



Internal Fraud -
While investigating through manual methods human error will be the highest leading cause of miss calculation while detecting the fraud. using AI or DeepLearning techniques the software can detect invisible patterns in the fraud and compares them with the previous data to give accurate results leading to lesser chances of false claims from the policyholders or their employees

Eligibility Fraud -
The most common instance in eligibility fraud is identity theft of policy holder or their dependent parties. using DeepLearning we can cross check the patient details from the huge variety of databases that include Aadhar, Voter ID, Pan card or any government ID Proofs. This will drastically reduce the chances of misusing identity of the policy user.

Application Fraud -
The AI software will compare the mandatory full body checkup to cross check any missmatch in information given by the policy holder.

Claim Fraud -
The advanced AI software detect the incorrect data or claim that is stated by the policy holder.

Proof of Concept

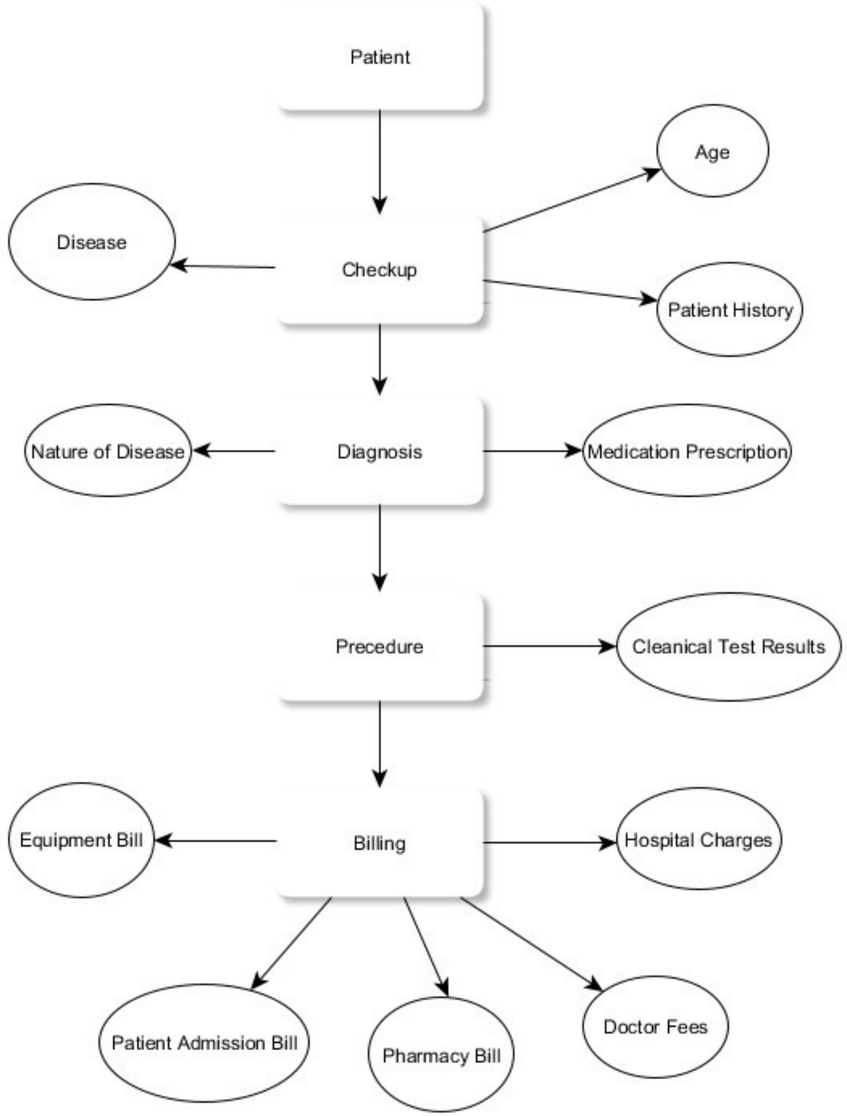
Introduction to Data and Methodology

INTRODUCTION TO DATA

The workflow analyses the Basic Stand Alone (BSA) Inpatient Public Use Files (PUF) named “CMS 2008 BSA Inpatient Claims PUF” with information from 2008 Medicare inpatient claims. This is a claim-level file in which each record is an inpatient claim incurred by a 5% sample of Medicare beneficiaries.

METHODOLOGY

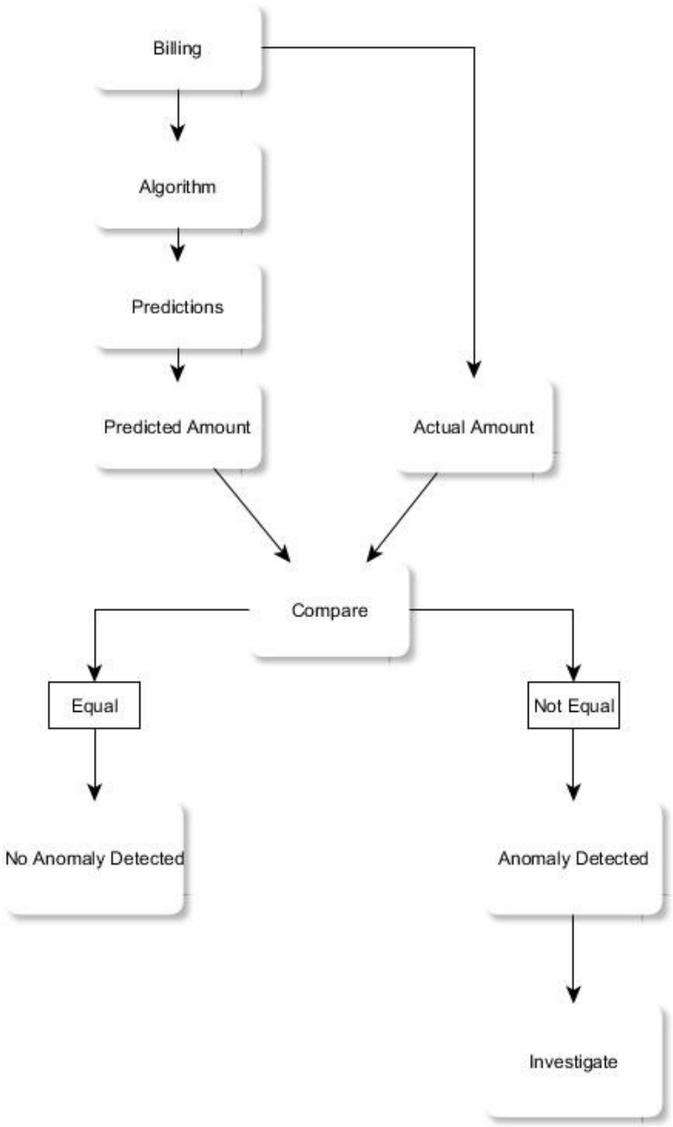
For this POC we try to explain how claim fraud can be detected and here we targeted the payment variable to find the fraud transactions that are already taken place. we have taken multiple variables to explain and analyze possible cases and outcomes.

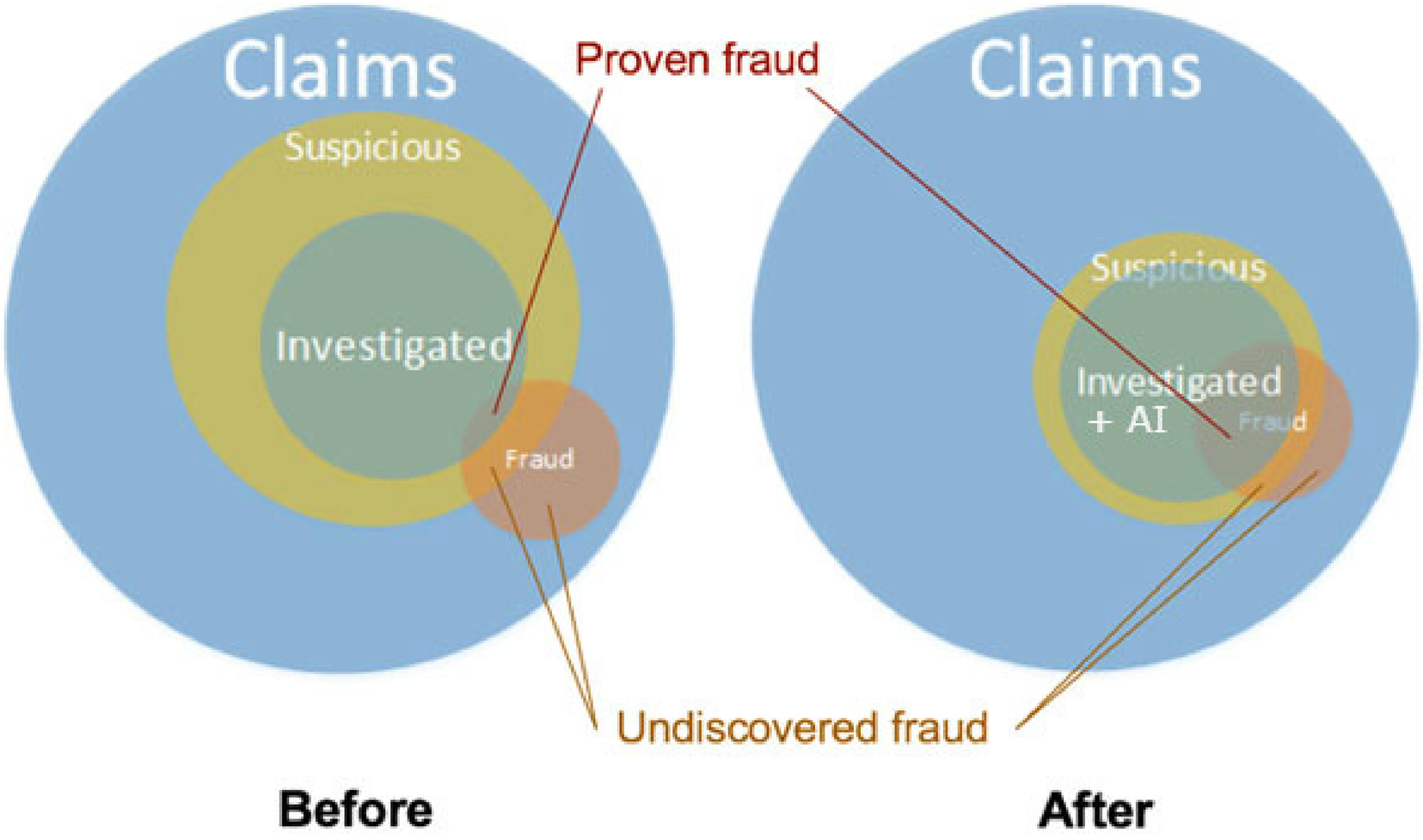


First here we take only required variables for the analysis in training and testing data and then given scoring for the values in the each variable. for example Beneficiary Gender Code has Female and Male as values we given scoring 1 for female and 0 male similarly for identifying the uniqueness of each patient record data. This scoring is also influence by the severity of the disease length of the procedure and total expencse of the entire procedure so that this is not only helpful for the algorithm but also for the human detection.

Now we taken Deep Learning algorithm to learn and predict the data. Deep Learning algorithms are very efficient for catching these type of sequence patterns in the data. We have to select which algorithm to use is based on type of the data and type of the problem. This algorithm work efficiently when trained with better and wide variety of data variables which results in almost 99% of accuracy.

With the help of our already available data we have made a few changes in the record to mimic the fraud that usually happens in the real time insurance fruad scenarios, this is our actual test data. Here we trained our algorithm with our training data and now it is ready to predict the payment variable with help of rest of the variables. We have given the test data to predict the payment variable so it gives predicted payment now we compare the predicted payment amount with actual amount if the payment in both variables is same then there is no fraudulent data. If there is any miss prediction then we can conclude that there is some incorrect data that has been recorded




Claims
Suspicious
Investigated
Fraud
Proven fraud
Claims
Suspicious
Investigated
+ AI
Fraud
Undiscovered fraud
Before
After

Real Time Scenario

Frauds have no constant patterns. They always change their behavior, so we need to use an semi supervised learning to detect the frauds. Fraudsters learn about new technology that allows them to execute frauds through online transactions. Fraudsters assume the regular behavior of consumers, and fraud patterns change fast. So, fraud detection systems need to detect online transactions by using semi supervised learning, because some fraudsters commit frauds once through online mediums and then switch to other techniques.

1) Focus on fraud cases that cannot be detected based on previous history or supervised learning.

2) We have to classify the data according to the Insurance policies so that we can avoid the incorrect fraud detections.

3) Need to make different types of techniques and algorithms for each type of fraud so that we can pin point each and every transaction like a filter.

Conclusion

In order to get results for the above problem that are highly accurate, we need to train our algorithms to learn and analyze various forms of insurance transactions and their outcomes. By making them more fine tuned to even detect any slight anomaly we can have greater chances of detecting the frauds as soon as they take place. AI will help fraud detection agents by finding the possible areas that fraud meant to happen and also we can get real analytics on fraud.

Contact Info

Mailing address

YDI Solutions Pvt Ltd,
Outer Ring Road, Marathahalli, Bengaluru, Karnataka,
560037.

Email address

contact@ydisolutions.ai

Phone number

+91 99161 72562