Unsupervised Anomaly Detection of Healthcare Providers Using Generative Adversarial Networks

Krishnan Naidoo, Vukosi Marivate

Unsupervised Anomaly Detection of Healthcare Providers using Generative Adversarial Networks

Krishnan Naidoo[1 [0000−0001−9509−5097]] and Vukosi Marivate[1,2 [0000−0002−6731−6267]]

[1] University of Pretoria, South Africa
[2] Council for Scientific and Industrial Research, South Africa
marionaidoo@gmail.com
vukosi.marivate@cs.up.ac.za

Abstract. Healthcare fraud is considered a challenge for many societies. Health care funding that could be spent on medicine, care for the elderly or emergency room visits are instead lost to fraudulent activities by materialistic practitioners or patients. With rising healthcare costs, healthcare fraud is a major contributor to these increasing healthcare costs. This study evaluates previous anomaly detection machine learning models and proposes an unsupervised framework to identify anomalies using a Generative Adversarial Network (GANs) model. The GANs anomaly detection (GAN-AD) model was applied on two different healthcare provider data sets. The anomalous healthcare providers were further analysed through the application of classification models with the logistic regression and extreme gradient boosting models showing good performance. Results from the SHapley Additive exPlanation (SHAP) also signifies that the predictors used explain the anomalous healthcare providers.

Keywords: Generative Adversarial Networks · Anomaly Detection · Healthcare Providers· Machine Learning · Deep Learning.

1 Introduction

In 2016, the global spend on health was US$ 7.5 trillion, representing close to 10% of global GDP [27]. Studies across Europe estimate around 30% have been lost to wasteful spending [14]. A study in 2016 by [25] confirms the financial value of fraud cases in Europe, with France leading the way with (€ 46.3M) of which 37% was committed by healthcare practitioners, 27% by health facilities and less than 20% by insured persons. Netherlands (€ 18.7M) fraudulent activity was mostly relating to wrongful billings, followed closely by UK (€ 11.9M) relating to fraud, bribery and corruption. In the United States healthcare fraud ranges from $80 billion to $200 billion [19] with some of reasons relating to improper coding, phantom billing, kickback schemes and wrong diagnosis.

In Africa, challenges like the lack of strong financial, processes and systems are some of the reasons contributing to healthcare fraud [20]. Reports suggests that approximately 3-4% of the R160 billion medical industry relates to fraudulent claims and abusive or wasteful healthcare costs in South Africa [4, 15]. Despite numerous efforts to solve for healthcare fraud, detection of these fraudulent activities within the healthcare sector is still a challenge due to poor data quality or lack of data [17, 24].

Due to the lack of confirmed fraud cases of healthcare providers, it is necessary to mention that GANs is a remarkable deep learning model in unsupervised and semi-supervised learning. Not only does the GANs model detect fraudulent activities and malicious users on online social platforms [7], they have been used to augment minority class that solve classification between fraudulent and normal samples [26]. Previous studies used traditional machine learning approaches to solve anomaly/fraud detection problems [2, 5, 23, 24], there has also been an increase in deep learning approaches to solve similar problems. These solutions have been predominately focusing on image problems and there is an opportunity for deep learning models to be applied within the health care domain to classify anomalies [12, 23, 26].

The objective was to build a single model across the various healthcare provider types to predict if a provider is fraudulent or not. This study uses a public data set from *Medicare Provider Utilization and Payment Data: Physician and Other Supplier* [4] and another private dataset from a *South African claim administration organisation.*

The remaining parts of this paper are structured as follows, Section 2 introduces the previous literature on healthcare provider cost abuse, discusses the various anomaly detection techniques and anomaly score. Section 3 presents our proposed methodology highlighting the GANS architecture, anomaly score function, algorithms, data sets used, data pre-processing and performance metrics. Section 4 discusses the results and implications. Finally Section 5 summarises the paper and proposes possible future work.

2 Literature Review

This section covers previous literature regarding the constructs, cost abuse and wastage, and anomaly detection models within the healthcare domain. Further to this, the literature was reviewed in the context of how machine learning has assisted in anomaly detection within the insurance and healthcare industry.

2.1 Healthcare Cost Abuse and Wastage

Healthcare fraud is an intentional deception to obtain unauthorised benefits. Research by [10] describes healthcare provider abuse as, a healthcare provider who practices, either directly or indirectly, in a manner that results in unnecessary costs to the provider. Abuse also relates to any healthcare provider that is not consistent in providing patients with medical services that are necessary,

inconsistent adherence to professionally recognised standards, and are not fairly priced [4, 24].

Recently a model proposed by [3] identified potentially fraudulent hospitals in the Brazilian public healthcare system. The methodology was based on analysing various procedures carried out across different hospitals in each city. The model makes use of a 2 step approach using the consumer anomaly detection using a K-nearest neighbours (kNN) algorithm and thereafter a consumer-provider transfer score showing the relationship between consumer and provider. In contrast, the kNN model was not effective with either very small or very big cities. Further challenges were experienced when the procedures were distributed across several cities.

Literature by [24] discusses how fraud detection could help combat healthcare provider cost abuse by securing the claim input process, checking on irregularities and analysing claim data sets to identify behavioural indicators of fraud. Anomaly detection can be used to identify potentially fraudulent behaviour which we discuss next.

2.2 Anomaly Detection

Anomalies are defined as patterns in data that do not conform to expected or normal behaviour [11]. The finding of such patterns is often referred to as anomaly detection [11, 29, 31]. Different anomaly detection techniques may be applied depending on the nature of the data. Usually if fully labelled data is available, supervised anomaly detection may be adopted. Data sets are considered as labelled if both the normal and anomalous data points have been recorded [29, 31]. When labels are not recorded or available, the only option is an unsupervised anomaly detection approach [31].

Research by [2] looked at supervised machine learning methods to detect fraudulent medicare providers across various states across America. The study evaluated three machine learning models indicating the decision tree and logistic regression as good performing models. The lack of fraud labels contributed to the imbalance of data and a random under-sampling strategy was employed to create the different class distributions. Sparsity of medical claim data and the availability of labelled fraudulent cases highlighted in [2, 10, 16, 23, 24] is a common challenge when solving for anomaly detection problems.

Canadian researchers [16] experimented on detecting anomalies using an unsupervised spectral ranking approach (SRA). The problem was approached as unsupervised learning which did not use labels when generating anomaly ranking using SRA. The study focused on detecting anomaly in the feature dependence using similarity kernels [16] . In addition, outcomes from the research highlighted the most important features to classify fraudulent claims are policy features, car types and cause of accident features.

The work of [5] includes a comparative survey over the last 20 years of outlier detection relating to fraud detection machine learning algorithms. The study indicates that Isolation Forest is a suitable model for efficiently identifying anomalies with good potential on scalability along with optimized memory utilisation

when using large data sets. In contrast, OCSVM is considered to be another good model for anomaly detection but does not perform well on large data sets and also can be challenging in tuning the input parameters [16].

Popular research across the healthcare and machine learning domains are either based on supervised learning [2], predefined medical rules [9], application of anomaly detection on medical images [21] or non healthcare data [28]. Further to this, research like [2, 3] also highlighted challenges like availability of data relating to healthcare providers, even if it is available there is not enough data or the data is not reliable since the providers themselves generate it [3].

Given the above, our methodology is a two step approach for anomaly detection. First, a GAN based approach was applied to identify the *anomaly* or *normal* labels. Second, the results from the deep learning model served as labels into identifying the features that contribute to the anomalous data points.

3 Methodology

Figure 1 illustrates the two step modelling approaches used describing the proposed methodology carried out. The first modelling step is a GANs model designed to identify the anomalous healthcare providers based on the reconstruction error. The second modelling step uses the anomaly labels in the supervised classification models and SHAP(SHapley Additive exPlanation) to explain the features contributing to the anomaly.

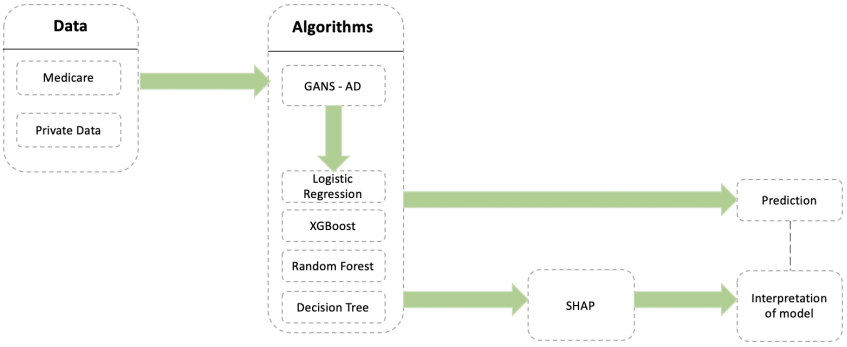

Fig. 1. Proposed methodology approach

3.1 Data Collection and Pre-Processing

To evaluate our anomaly detection approach, we describe the datasets and preprocessing in detail.

Medicare Dataset: The data for the current study is a public data set from the Centers for Medicare and Medicaid Services (CMS) for the 2016 calendar year only [4]. The *Medicare Provider Utilization and Payment Data: Physician and Other Supplier* contains payment and claims data with information on services and procedures provided to claimants and beneficiaries. The medicare dataset is aggregated containing 1,053,958 samples with 70 features. As part of the data pre-processing phase, a one-hot encoding representation was applied on categorical features. Thereafter, standardised scaling was applied and highly correlated features was removed. The final output from the pre-processing step that was used in the GANs model contained 91 features with a combination of categorical features representing the practitioner type, type of injury and continuous features representing payment across beneficiaries and injury types.

Private Dataset: The research also used data from an organization for which access has been granted to carry out the research. The required data was obtained from a South African company that performs the administration of claims occupational injuries and diseases according to the South African Compensation for Occupational Injuries and Diseases Act (COIDA). The data was aggregated to healthcare provider level with features created to represent financial and injury information. Thereafter the similar pre-processing step applied on the Medicare data set was also applied on the private data set. The final output from the pre-processing step was used in the GANs model contained 95 features.

We applied our modelling approach to both data sets. The data has been modified to mask the healthcare providers details in the results, and examples shown in this paper due to ethical and privacy issues.

3.2 Algorithms

Both data sets described in Section Three does not contain any labels. Unlike other machine learning algorithms, that requires a vast amount of labelled data in order to generalize well, GANs can be trained with missing data [1, 21] and can also improve the performance of classifiers when limited data is available. The labels were defined by the application of a GANs with a "feature-matching" anomaly score. Thereafter several classification models (Random Forest, Decision Trees, Logistic Regression and Extreme Gradient Boosting) were applied to get a deeper understanding of how the features contribute to the anomalous labels.

Generative Adversarial Networks (GANs) algorithm consists of two adversarial networks, a generator G and a discriminator D [8]. In the context of anomaly detection, the first term in Equation 1 ($[\log D(\mathbf{x})]$) is the real distribution of data that passes through the discriminator (normal data). The discriminator tries to maximize these data samples to 1. The second term term in Equation 1 ($[\log(1 - D(G(\mathbf{z})))]$) represent data from random input that passes through the generator, which then generates fake samples which is then passed through the discriminator to identify the anomaly. In this term, discriminator tries to maximize it to 0. So overall, the discriminator tries to maximize the

function V. Similarly, the task of generator is exactly opposite, it tries to minimize the function V so that the differentiation between normal and anomalous data is at a minimum.

$$\min_{G}\max_{D} V(D.G) = \mathbb{E}_{\mathbf{x}\sim p_{data}(x)}\left[\log D\left(\mathbf{x}\right)\right] + \mathbb{E}_{\mathbf{z}\sim p_{\mathbf{z}}(z)}\left[\log\left(1 - D\left(G\left(\mathbf{z}\right)\right)\right)\right] \tag{1}$$

Detection of an anomaly: The GANs algorithm labelled data as normal or anomalous through the use of a loss function called the *anomaly score*. The *anomaly score* is calculated for every evaluation between normal and generated samples in the training process [21,28]. The *anomaly score* is represented by the following equation:

$$A(x) = (1-\lambda)\cdot \mathbf{G}(x) + \lambda \cdot \mathbf{D}(x) \tag{2}$$

In Equation 2 the generator score $\mathbf{G}(x)$ and the discrimination score $\mathbf{D}(\mathbf{x})$ are defined by the *generator loss* $\mathcal{L}_G$ and the discrimination loss $\mathcal{L}_D$ respectively. For a given data sample x, a high anomaly score of $A(x)$ indicates possible anomalies within the sample. The evaluation criteria for this is to a threshold (ϕ) the score, where $A(x) > \phi$ indicates anomaly. In the current study the threshold is set to 90%.

Classification Algorithms: Four binary classification algorithms were applied in the second part of the study to give interpretability to the anomalies. The algorithms applied include the logistic regression(LR), extreme gradient boosting (XGB), random forest (RF) and decision tree (DT) [22]. These algorithms are summarised highlighting their core capability.

Logistic Regression(LR) is a classification algorithm that is used to predict the probability of a binary dependent variable. In the current context, the dependent variable contains data coded as 1 (anomaly) or 0 (normal). *Extreme Gradient Boosting (XGB)* is a powerful machine learning technique for classification, regression and ranking problems [18] which produces a prediction model in the form of an ensemble decision tree [18]. The XGB model is built in a multi step approach where each step, introduces a new weak learner to compensate the shortcomings of the existing weak learners [18]. *Random Forest (RF)* is a tree constructed algorithm from a set of possible trees with random features at each node. Random forest can be generated efficiently and the combination of large sets of random trees generally leads to accurate models to detect anomalies [22]. Moreover, the random forest algorithm has been used in this study due to its versatility in being applied to large data sets and feature importance [6]. *Decision Tree (DT)* is a simple and intuitive algorithm that utilize a top-down approach in which the root node creates binary splits until a certain criteria is met [6]. In the current context of anomaly classification, the decision tree model outputs a predicted target class (anomaly or normal) for each terminal node

produced. Decision Trees automatically reduce complexity, selection of features and the predictive analysis structure is understandable and interpretable [22].

The LR, XGB, RF and DT algorithms are successful in detecting anomalies [6, 18, 22] however their main use in the current study is their ability to generalize, feature selection, interpretability [6, 18, 22, 30] and further explain how the features contribute to the anomalous healthcare providers. This explanation was further achieved through the use of SHapley Additive exPlanation (SHAP) [13].

SHAP(SHapley Additive exPlanation) objective is to explain the prediction of anomalous healthcare providers by computing the contribution of the features to the prediction. The explanation method within SHAP computes Shapley values from game theory [13] which indicates how the distribution of the anomaly label (the prediction) among the predictors(features). In the context of the current study, SHAP provided a unified approach for the interpretability of the features in detecting anomalies across healthcare providers. The SHAP framework was applied to assist in explaining the accuracy, consistency, stability, certainty, feature importance and representation of the features.

4 Results and Analysis

In this section, we discuss the predication results of our proposed methodology on the two data sets. First, we discuss the generative capability of the GANs and the appropriateness of the data generation and scoring approach for anomaly detection. Thereafter, we discuss the four classification models and SHAP results.

4.1 Unsupervised Label Generation

Generation of realistic data The challenge in the study is the lack of fraud labels across the data sets which plays an important role in measuring model performance and accuracy in machine learning models. This simplify the current study to adopt a GANs approach to generate fraud labels that is used as the ground truth. The trained GANs model generates realistic data across the different features. The generated data is conditioned by sampling from latent representations z discussed in Section Three. The data distribution for the generated data and real data is represented for one feature across the two data sets (see Figure 2). The distribution of the generated data show some similarities to the real data and also points that is vastly different from the normal data points.

Detection of Fraud Labels: Figure 4 shows the anomaly detection based on the anomaly score from the GANs algorithm (Equation 2). The distributions of the anomaly score (Figure 3 and 4) show that both components of the proposed adversarial score are suitable for the classification of normal and anomalous samples.

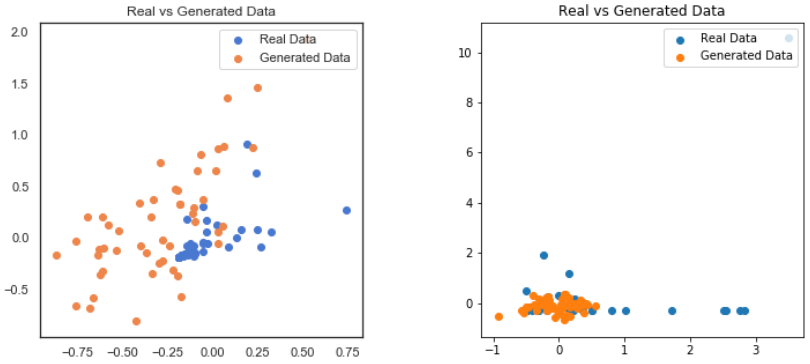

Fig. 2. Real vs Generated data across a) Medicare and b) private data set

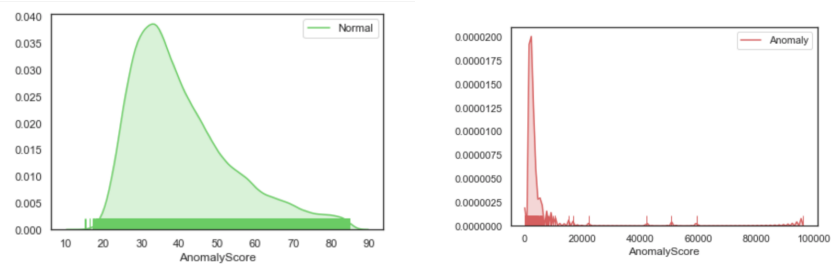

Fig. 3. The anomaly scores on Medicare data set for a) normal healthcare providers is at the lower end (below 100) whereas b) anomalous healthcare providers is spread across low and high anomaly scores

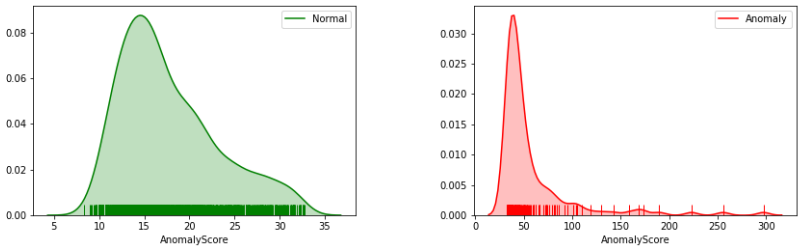

Fig. 4. The anomaly scores on private data set for a) normal healthcare providers is at the lower end (below 100) whereas b) anomalous healthcare providers have higher anomaly scores

4.2 Model Interpretation

In the following subsection, the results are based on the model performance from the Logistic Regression, Random Forest, Decision Tree and Extreme Gradient Boosting algorithms. The supervised modelling process used 60% of instances for training and the remainder in test (20%). Due to the imbalance of data between normal and anomalous labels under sampling was applied during the training process. Table 1 highlight the results from the supervised classification-based models.

The performance across all the models exceeds 90% on the private data set with the two high performing models based on Area Under Curve(AUC) was LR (97.4%) and XGB (90.3%) respectively. On the Medicare data set the performing model based on AUC was the LR (75.7%) followed by the XGB (74.7%). Table 1 shows the LR results on both data sets with regards to AUC, 75.7% and 97.4% respectively. With sensitivity and specificity rates of 81.3% and 70.1% for the Medicare dataset, and 99.6% and 95.2% for the private dataset. The high sensitivity rate across the two data sets indicates the LR model does well in classifying the anomalous labels identified by the GANs model.

In the context of the current classification problem, a higher sensitivity value would be preferred in identifying anomalous healthcare providers. The second part of the study was aimed to identify the key features contributing to the anomalies so the necessary controls can be in place. Further to this, the results indicates that the supervised classification algorithms performed well across the private data however the results on the Medicare dataset is lower. This can be attributed to the imbalance of labels in the dataset.

Table 1. Model results across the Medicare and private dataset

	Medicare				**Private**			
Model	Accuracy	Sensitivity	Specificity	AUC	Accuracy	Sensitivity	Specificity	AUC
LR	**0.802**	**0.813**	0.701	**0.757**	**0.992**	**0.996**	**0.952**	**0.974**
CART	0.7	0.702	0.688	0.695	0.972	0.99	0.812	0.901
XGB	0.759	0.762	**0.731**	0.747	0.976	0.994	0.812	0.903
RF	0.787	0.797	0.689	0.743	0.972	0.993	0.783	0.888

4.3 SHAP

SHAP analysis was conducted and shows the features which push the base value to the model output. Figure 5 and 6 shows features pushing the prediction higher (in red) and those pushing the prediction lower (in blue).

Figure 5 shows the features in Medicare containing high values for total unique beneficiaries, number of HCPCS and beneficiaries between 65 and 74 indicating major impact on increasing the prediction. In addition, low feature values for total unique beneficiaries, number of HCPCS, beneficiaries between 65 and 74 indicate these features decreases the prediction value.

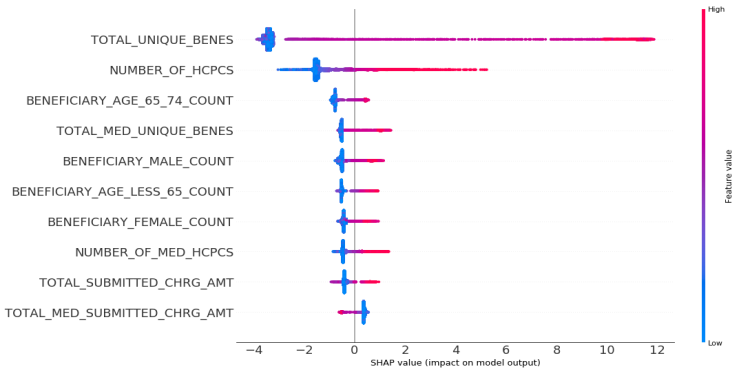

Fig. 5. SHAP Feature Summary - Medicare

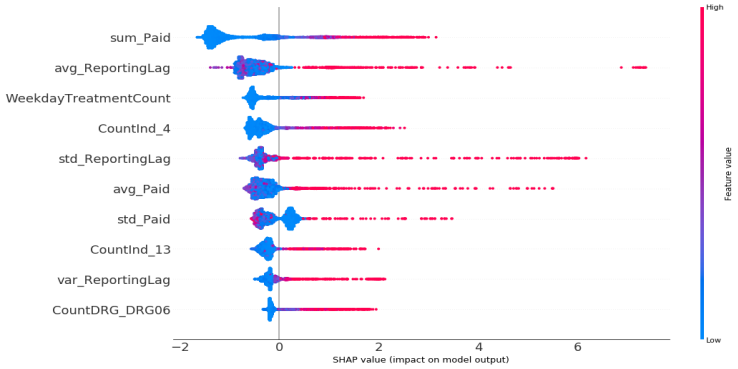

Fig. 6. SHAP Feature Summary - Private

Figure 6 shows the features in the private dataset containing high values for reporting lag, days to end of month and payment have a major impact on increasing the prediction, while low feature value for reporting lag decreases the prediction. Overall features like reporting lag, value of payments and number of injuries for a specific injury group are important features in determining if a healthcare provider is fraudulent or not.

5 Conclusion

The study proposed an anomaly detection model based on generative adversarial networks. By training a generator and discriminator model, anomalies were identified from unseen data based on unsupervised training of a model. The labels generated from the GANs model was used as the ground truth in the supervised classification models to gain further insight on the features contributing to the anomalous healthcare providers. Across the four supervised models evaluated,

the logistic regression was the best performing classifier across the two data sets. This methodology applied on similar data sets can offer subject matter experts the ability to detect anomalous healthcare providers with a high degree of accuracy.

Results showed the GANs model identified anomalous healthcare providers and the use of SHAP explained predictors. This approach can be beneficial to future researchers where availability of fraud labels is a challenge. Future studies could solve some of the limitations in the evaluation of the model. The evaluation of label generation in unsupervised models is a challenge and solving this problem would give researchers the opportunity of evaluating the labelling method more precisely. Furthermore explore the use of SHAP directly on deep learning models to better explain feature importance and interpretability.

References

1. Akcay, S., Atapour-Abarghouei, A., Breckon, T.P.: GANomaly: Semi-Supervised Anomaly Detection via Adversarial Training. Ph.D. thesis (2018)
2. Bauder, R.A., Khoshgoftaar, T.M.: The Detection of Medicare Fraud Using Machine Learning Methods with Excluded Provider Labels. The Thirty-First International Florida Artificial Intelligence Research Society Conference pp. 404–409 (2017)
3. Carvalho, L.F., Teixeira, C.H., Meira, W., Ester, M., Carvalho, O., Brandao, M.H.: Provider-Consumer Anomaly Detection for Healthcare Systems. Proceedings - 2017 IEEE International Conference on Healthcare Informatics, ICHI 2017 pp. 229–238 (2017)
4. CMS: CMS: Research, Statistics, Data and Systems (2014), https://www.cms.gov/research-statistics-data-and-systems/research-statistics-data-and-systems.html
5. Domingues, R., Filippone, M., Michiardi, P., Zouaoui, J.: A comparative evaluation of outlier detection algorithms: Experiments and analyses. Pattern Recognition pp. 406–421 (2018)
6. Dora, P., Sekharan, G.H.: Healthcare Insurance Fraud Detection Leveraging Big Data Analytics. International Journal of Science and Research pp. 2073–2076 (2015)
7. Goix, N.: Machine Learning and Extremes for Anomaly Detection-Apprentissage Automatique et Extrêmes pour la Détection d'Anomalies Spécialité "Signal et Images" présentée et soutenue publiquement par (2016)
8. Goodfellow, I.J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., Bengio, Y.: Generative Adversarial Networks. Advances in neural information processing systems pp. 1–9 (2014)
9. Herland, M., Bauder, R.A., Khoshgoftaar, T.M.: The effects of class rarity on the evaluation of supervised healthcare fraud detection models. Journal of Big Data (2019)
10. Joudaki, H., Rashidian, A., Minaei-Bidgoli, B., Mahmoodi, M., Geraili, B., Nasiri, M., Arab, M.: Using Data Mining to Detect Health Care Fraud and Abuse: A Review of Literature. Global Journal of Health Science pp. 194–202 (2014)
11. Lazarevic, A., Ertoz, L., Kumar, V., Ozgur, A., Srivastava, J.: A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection. Army High Perform- ance Computing Research pp. 25–36 (2013)

12. Liu, E., Ahmad, M.A., Eckert, C., Nascimento, A., De Cock, M., Padthe, K., Teredesai, A., Mckelvey, G.: Automatic Detection of Excess Healthcare Spending and Cost Variation in ACOs. SIAM (2018)
13. Lundberg, S.M., Lee, S.I.: A Unified Approach to Interpreting Model Predictions Scott. Neural Information Processing Systems Conference pp. 426–430 (2012)
14. McDaid, D., Merkur, S., Maresso, A.: EuroHealth Report. European Observatory on Health systems and Policies pp. 1–44 (2011)
15. Molefe, P.: CMS News The Council for Medical Schemes'. Tech. rep. (2018)
16. Nian, K., Zhang, H., Tayal, A., Coleman, T., Li, Y.: Auto insurance fraud detection using unsupervised spectral ranking for anomaly. The Journal of Finance and Data Science pp. 58–75 (2016)
17. Nicolaides, A., De Beer, F.: Practitioner Ethics , Medical Schemes and Fraud in the South African Private Healthcare Sector. Medical Technology SA pp. 1–11 (2017)
18. Niu, X., Wang, L., Yang, X.: A Comparison Study of Credit Card Fraud Detection: Supervised versus Unsupervised. Association for the Advancement of Artificial Intelligence (2019)
19. OECD Publishling: Health at a Glance: Europe 2018: State of Health in the EU cycle (2018)
20. Organization, W.H.: Prevention not cure in tackling health-care fraud. Bulletin of the World Health Organization pp. 853–92 (2011), https://www.who.int/bulletin/volumes/89/12/11-021211/en/
21. Schlegl, T., Seeböck, P., Waldstein, S.M., Schmidt-Erfurth, U., Langs, G.: Unsupervised anomaly detection with generative adversarial networks to guide marker discovery. Information Processing in Medical Imaging pp. 146–147 (2017)
22. Sekhar, C.R., Minal, Madhu, E.: Mode Choice Analysis Using Random Forrest Decision Trees. Transportation Research Procedia pp. 644–652 (2016)
23. Shi, Y., Sun, C., Li, Q., Cui, L., Yu, H., Miao, C.: A Fraud Resilient Medical Insurance Claim System. Proceedings of the 30th Conference on Artificial Intelligence (AAAI 2016) pp. 4393–4394 (2016)
24. Thornton, D., Brinkhuis, M., Amrit, C., Aly, R.: Categorizing and Describing the Types of Fraud in Healthcare. Procedia Computer Science pp. 713–720 (2015)
25. Vincke, P.: Fighting Fraud & Corruption in Healthcare in Europe: a work in progress. Tech. rep. (2016)
26. Wang, Y., Xu, W.: Leveraging deep learning with LDA-based text analytics to detect automobile insurance fraud. Decision Support Systems pp. 87–95 (2018)
27. Xu, K., Soucat, A., Kutzin, J., Brindley, C., Maele, N.V., Touré, H., Garcia, M.A., Li, D., Barroy, H., Flores, G., Roubal, T., Indikadahena, C., Cherilova, V., Siroka, A.: Public Spending on Health: A Closer Look at Global Trends. Tech. rep. (2018)
28. Zenati, H., Foo, C.S., Lecouat, B., Manek, G., Chandrasekhar, V.R.: Efficient GAN-Based Anomaly Detection. ICLR pp. 1–7 (2018)
29. Zhang, C., Song, D., Chen, Y., Feng, X., Lumezanu, C., Cheng, W., Ni, J., Zong, B., Chen, H., Chawla, N.V.: A Deep Neural Network for Unsupervised Anomaly Detection and Diagnosis in Multivariate Time Series Data. Association for the Advancement of Artificial Intelligence (2018)
30. Zhou, X., Cheng, S., Zhu, M., Guo, C., Zhou, S., Xu, P., Xue, Z., Zhang, W.: A state of the art survey of data mining-based fraud detection and credit scoring. MATEC Web of Conferences (2018)
31. Zoppi, T., Ceccarelli, A., Bondavalli, A.: On algorithms selection for unsupervised anomaly detection. Proceedings of IEEE Pacific Rim International Symposium on Dependable Computing, PRDC pp. 279–288 (2019)