Mapana – Journal of Sciences
2024, Vol. 23, Special Issue 3, 81-101
ISSN 0975-3303|https://doi.org/10.12723/mjs.sp3.5

The Need and Importance of Augmented AI/ML Systems for Health Claims Fraud Detection

Parul Naib*, Sudha Chandrashekar* and S D Gupta*

Abstract

Artificial Intelligence (AI) and Machine learning (ML) systems are increasingly being used to solve basic day-to-day problems. Chatbots such as Alexa and Siri play a big role in our day-to-day life with our reliance on these systems increasing by the day. The use of AI and ML systems is being increasingly explored, in fraud detection. particularly for the detection of fraud health insurance claims submitted by providers. Recently, several studies have leveraged AI/ML techniques to develop health claims fraud detection models with close to 100% accuracy rates. These models are fully reliant on the machine for feature selection, training from the existing labelled data, and providing the final output with very little human intervention. This paper looks at the limitations of the deep learning-based AI and ML models in the case of health claims fraud detection, and the associated challenges and implications. We then define an integrated AI/ML strategy augmented by human intelligence for prompt and comprehensive fraud control to address the challenges and how organisations can use AI/ML responsibly for fraud detention without impacting the patient experience and health outcomes.

Keywords— Fraud, Artificial intelligence, Machine learning, Health Insurance, claims, healthcare fraud

I. Introduction

* Department of Public Health, IIHMR University, Jaipur, India; parul.j19@iihmr.in; sudhashreec@yahoo.co.in; sdgupta@iihmr.edu.in

The use of AI/ML in everyday life is quite pervasive, to the extent that we do not even realise how much our lives are dependent on it. Right from using Alexa to getting a forecast on the weather to using a GPS-based navigation system to identify the fastest route to reach the office, we depend on AI/ML systems to guide, recommend and advise us to make our life easier and smoother. AI/ML has become an integral part of how we see and perceive things around us, with anyone having a smartphone being a potential user of AI/ML. As per the GSMA State of Mobile Internet connectivity report 2020, 3.8 billion people were using mobile internet by 2019 and estimated that there would be 1.8 billion 5G connections by 2025. Further, three-quarters of all current mobile internet users live in low- and middle-income countries (GSMA, 2020).

AI/ML systems can scan through millions of data records in fractions of seconds, analysing an individual's historical purchase/preference history, comparing it to other users and creating clusters of similar individuals to come up with a personalised recommendation for each one [2]–[4].

Fraud Health Claims Detection using AI/ML

Recently, the use of AI/ML techniques in fraud detection has increased substantially, particularly for health insurance claims. Several research articles have looked at the development of machine learning models for this such as Neural networks, Random forests, Support Vector Machines, Bayesian Models etc. These models boast a high accuracy and precision in being able to detect and classifying fraud claims [5]–[12]. Recently, the use of deep learning models has become increasingly popular, given the high accuracy rates that can be achieved [13]–[15], some models even claim to reach an accuracy of 99.99%.

The use of AI/ML in this area, however, comes with its own set of challenges, given the complexity and diversity of health systems, alternative medical treatments that may be applicable for the same ailment depending on the patient's pre-existing medical conditions and the evolving nature of diseases and adoption of new treatment therapies. For instance, the emergence of the COVID-19 pandemic and the associated set of treatment therapies, drugs, and vaccines disrupted the entire functioning of health systems and resulted in significantly different trends in claim patterns as opposed to previous years [16]–[18]. Further, as several studies have pointed out, health systems themselves have certain inherent limitations which make them particularly vulnerable to fraud and abuse by providers- in the form of information asymmetry between the doctor and payer about the true medical condition of the patient, the incentive incompatibility in case of fee-for-service models which result in excess billings/ treatments and uncertainties and complexity of health systems due to multiple stakeholders and the emergence of new infections, diseases etc.[19]–[23].

Before proceeding, it would be helpful to look at the key types of health insurance fraud as defined in the existing literature [24]–[27]. The key fraud types in the case of healthcare – (1) Ghost billing or billing for claims where treatment has not been provided, (2) Upcoding or billing for a higher-priced procedure than what was performed, (3) Medically unnecessary procedures: Prescribing investigations or treatments which are not required or admitting patients in the hospital when they can be managed as an outpatient, (4) Unbundling: Charging separately for services that are already included in the procedure cost and (5) False referrals for kickbacks

All these different types of fraud have certain nuances and need to be addressed using different approaches to enable the machine to learn and train from the data.

Machine Learning Models used in Fraud Detection

The area of fraud detection has been using machine learning algorithms for the past few years now. In most industries, genuine transactions account for a majority of the transactions, and events of fraud are few and rare. Machine learning models help to identify the patterns in these rare events and are frequently used for prediction and analysing key drivers of fraud. [28]–[30]. Some of the models used are:

Logistic Regression: The use of Logistic Regression for fraud detection is being done for several decades now. Logistic Regression models are often used in the case of binary classification where the variable to be predicted takes binary values. This makes it an ideal candidate to identify fraudulent transactions by assigning a binary value of 1 or 0 to the transactions to indicate if they are fraudulent or not. These models help to assign probabilities to each claim about the likelihood of it being a fraud [31], [32].

Decision Trees: Similar to Logistic regression models, decision trees can also help in the classification of fraud vs genuine transactions and are particularly helpful when we are working across different segments- such as different geographies, different types of industries etc which may have different patterns of fraudulent activities and hence different independent variables which impact the fraud, which can be used as different nodes of a decision tree and obviates the need to develop separate models for each of these segments [11], [33], [34].

Deep Learning such as Neural Networks: The use of Neural networks have been fairly recent, these deep learning models operate in the form of a black box, on a system of layered neural networks, which operate similar to human brain neurons. The neural networks act as 'input receptors' to access the structured or unstructured data (medical images, clinical notes, diagnostic reports etc), the information is then processed to identify the underlying patterns in the labelled data to identify fraud vs genuine transactions. Since deep neural networks leverage several hidden layers of such networks, their accuracy in the classification of transactions as fraud and non-fraud is usually very high and further improves as they are trained on more and more labelled data [13], [35].

We now proceed to look at some of the key challenges and limitations in applying AI/ML techniques to fraud detection in health claims.

Challenges in applying Machine Learning to Healthcare Fraud Detection

Machine Learning Techniques require accurately labelled data: Machine learning models and algorithms learn how to categorise and classify claims as fraud or genuine, looking at historical trends, analysing patterns and characteristics for these categories and the key differentiating factors between them. This requires correct labelling of the historical data- claims as fraud and genuine. However, several research studies have established that a bulk of healthcare fraud goes undetected [23], [36], [37]. Unlike fraud in financial services like banking or credit cards, where it is easier for a customer to detect and report fraud transactions by looking at the account statement, detecting healthcare fraud is not as straightforward due to various reasons. Firstly, most patients do not receive an explanation of benefits (EOB) unless the claim is denied, which makes it difficult to keep track of when fake claims may be getting submitted and approved using the individual's policy. Further, given the information asymmetry between the provider and patient /payer regarding the patient's true medical condition and the type and level of care needed, it is difficult for the patient to identify if unnecessary or inappropriate treatments are performed or even if the procedure billed for is different from the one performed given the complexity of medical terminology. Thus, a bulk of healthcare fraud goes undetected, and transactions that are being used to train the machine as apparently 'genuine', may be fraud, making the input data set unreliable. Inputting this incorrectly labelled data into the model may result in missing out on important patterns of the fraud claims.

Accuracy of Input data: The power of the AI/ML algorithms is determined to a great extent by the quality of data being submitted. Till recently, claims were submitted in the form of paper records or had to be coded manually which led to coding errors and omissions. This greatly impacted the actual in-production accuracy of the fraud detection models. Further, most providers especially in developing countries still use handwritten notes and prescriptions which are not easy for the machine to read [38]. Recent advancements in electronic health records address that to some extent, however, the adoption has been slow and the capability to integrate and synthesise the health data continues to be a challenge.

Deep Learning models and Black box environment: Several research studies have highlighted the challenges of deep learning models and how they operate, in a 'black-box environment' making it difficult to understand how the model was developed at each step (due to several hidden layers), including how the features that were selected to distinguish between the fraud and non-fraud claims. [39]–[41]. In this case, it becomes difficult to know how the model determined the 'fraud ' transactions and then explain them clearly to providers. If providers perceive that claims are denied without a valid justification, it leads to a breach of trust between provider and payer leading to denial of care and adverse patient health outcomes [42], [43].

Non-translatability of results into actions: Most deep learning-based studies only provide the accuracy without really specifying the individual factors driving the fraud or details of the patterns observed in health claims, why the transactions were classified as fraud etc [13], [14], [44]. Without understanding the key factors that influence the fraud, it is difficult for payers to understand how to modify their processes and policies, and the kind of medical protocols to introduce to control the fraud.

Inconsistency with payer objectives: Another risk associated with the complete reliance on machine-based algorithms is that they may make decisions and take actions which may not be fully consistent with the payer organisations' objectives. Machines typically tend to do unconstrained optimisation which often leads to local optima being achieved, which may not be the global optimal (i.e. best across all organisational objectives) from a payer perspective. For eg., An automated AI engine may start pending or declining or high-risk transactions that it classifies as fraud which may serve the objective of fraud control, but may impact other objectives such as optimising the patient and provider experience.

The use of results coming from a black box model has serious implications when it comes to a sensitive area such as health insurance as adjudication of healthcare claims needs to be very precise. An incorrect decision (Type 1 or Type 2 error) of misclassifying a genuine claim as 'fraudulent' or vice versa has serious implications for the stakeholders involved.

The evolving nature of healthcare fraud: Fraud in any industry is dynamic in nature and keeps evolving. Similar to a 'cat and mouse game', the fraud manager keeps trying to identify fraud and close loopholes to nab the fraudster, while fraudsters keep thinking of new ways to commit the act once the previous modus operandi is exposed. Similarly, providers also try to identify newer ways to commit the fraud and cover up their actions, often colluding with other players and making it more difficult to detect. For instance. In the 2020 National Healthcare fraud takedown, the US Office of Inspector General (OIG) charged several different entities ranging from telemedicine executives, the owners of durable medical equipment (DME) companies, genetic testing laboratories, pharmacies, and medical practitioners, for their alleged participation in health care fraud schemes worth $6 billion. Over $4 billion of the fraud losses had occurred from a relatively new type of healthcare fraud related to telehealth. [45]. In such scenarios, a model which has been trained on past fraud trends may not be able to identify new types of frauds as they emerge and evolve.

Non-generalisability in case of emergence of new disease trends/ infections: There is a lot of uncertainty in the health systems owing to the emergence of new diseases, recurrence of infectious diseases, and new variants of previously identified pathogens. This makes it further difficult for the machine to adapt and past learnings of the model cannot be directly applied to these new situations. For eg., Machine learning models had not seen claims submitted for COVID in the past and that too in such huge numbers. Thus it may be easy for the machine to confuse such claims as a new fraud trend or identify hospitals reserved for COVID treatment as 'outliers'.

Full autonomy to AI: The need for ensuring that these systems 'behave' in the way they are supposed to and not get out of control is equally important. Giving full autonomy to AI/ ML systems to make a decision is fraught with several risks, especially in the case of time-sensitive matters of healthcare where a single incorrect adjudication decision may result in either denial of care or compromising the quality of care or passing on the payment burden on the patient. In the recent past, adverse events like where FB's chatbots going rogue or auto-pilot vehicles not taking timely decisions have resulted in several accidents including flight crashes. [46], [47]. Thus, giving full autonomy to AI/ ML models in a sensitive area involving patient health is extremely risky.

Implementing Effective AI/ML systems in Health Claims Fraud Detection- An Augmented Approach:

Given the challenges mentioned above, it becomes adequately clear that the use of the AI/ML approach must be reinforced by human experts as well. While Artificial Intelligence and Machine learning can help to significantly ease the burden of repetitive tasks and enhance the user experience, they must be developed with a good understanding of the domain and the problem statement to which it is applied. In the case of fraud detection, the use of AI and ML must be augmented with the knowledge of data scientists and experts of domain experts. This will also ensure that the final ownership and accountability of the actions emanating from the models for fraud control remains with humans and can be corrected. [48]–[50]

Data Collection: Right at the stage of data collection, it is advisable to have electronic health records, with the procedure-specific mandatory medical information (such as Diagnosis codes, Procedure codes and the necessary investigations etc) to be directly entered into the claims system, rather than getting the information in paper documents or uploaded images. [31]. Standardised formats for documents that are considered mandatory for the claims processing should be developed in the claims system and auto-populated to create standardised diagnostic reports, discharge summaries etc. This will help to create structured and unstructured data which can be analysed by the machine as opposed to handwritten documents. Most developed countries are now moving to the leveraging of electronic health records -In South Korea, the EHR adoption rate has steadily increased from 15.1% in 2010 to 58.1% in 2015, in Japan the same increased from 21% in 2008 to 53% in 2014. [51], [52] Between 2007 to 2018, the average adoption rates of hospitals in China increased from 18.6% to 85.3%, Similarly in Germany, the usage of EHRs in German hospitals increased from 39.9% in 2007 to 68.4% in 2017 [53] while in the US, it increased from 9.4% to 96% from 2008 to 2017. [54]. Natural language processing algorithms can then analyse these electronic health records in a faster and more effective manner. Automated NLP systems can also reduce the administrative burden on providers by generating automated clinical notes in the IT system instead of typing long medical/OT notes.[55], [56]

Data Ingestion and Treatment: During this stage, data checks and validations are performed to ensure that missing values and outliers get identified. Missing Value treatment using median imputation and

Outlier treatment is performed to ensure that the data is clean. The data must be stored in a safe environment on a secure cloud or VPN-based servers to ensure its confidentiality. The machine should run on a backup version of the data and not on the original data itself with no ability to write or update any data. At this stage, any new trends of diseases must be flagged so that the machine can be trained separately on those. Data gaps such as missing ICD-codes/ CPT codes must be flagged so that they can be inputted using the documents uploaded. Figure 1 below provides a summary view of the data pre-processing steps consisting of Outlier and missing value treatment to ensure that the appropriate records are included in the analysis. Various data elements from different platforms such as patient, hospital, claims, pharmacy etc are integrated to get a comprehensive view of the entire interaction so that new patterns can be immediately identified and flagged.

Feature selection and segmentation: Care must be taken at the feature selection stage itself to input variables based on the domain knowledge and expertise. Though the machine may be capable of identifying differentiating features, the domain-specific knowledge should be provided by the medical experts to identify those which make logical sense in the business context. This in turn helps to identify factors that may be correlated spuriously and reduce false positives. Once these factors are selected by experts, the same can then be inputted into the machine to identify those which provide the best differentiation between the fraud and non-fraud transactions. In case of healthcare fraud, given the various nuances, the following segmentation strategies may be adopted:

By specialities: Given that different specialities/procedures have different criteria and nuances in terms of the level of care needed (inpatient or outpatient), length of stay, and nature of treatment (surgical or medical), it is good to look at the underlying patterns for each speciality separately to identify the fraud. This would help to identify specific patterns, for instance, Cardiology claims often require surgical interventions and a long length of stay. These are significantly different from those of medical management claims such as fever etc which may be either outpatient/or with a few days of inpatient care and require no surgery or those of Oncology which may require multiple sessions of chemotherapy over a prolonged period. Each speciality thus has its own underlying patterns of claims. It is essential to factor in such patterns while developing models.

By Regions: Different geographical regions also tend to show differences in fraud trends and rates. This may be so, since different regions may have different demographic populations with different disease burdens. For example developed countries such as the USA, UK, and Japan have a higher proportion of the elderly population, and lifestyle-related diseases are more predominant as compared to tropical developing countries such as India, Kenya, and Bangladesh where the population is younger but infectious diseases such as malaria, TB, typhoid are more common. Thus, regional variations also need to be accounted for in the models.

By Provider Type: Healthcare facilities range from small physician clinics, community health centres, mid-sized hospitals, and single speciality providers to large multi-speciality hospitals, each having different trends in claim submission. Thus separate models may be needed depending on the provider type especially to identify outliers and peer comparisons.

Accounting for seasonal variation: It may also be important to account for seasonality in models, given that certain infectious diseases such as dengue, malaria, and certain flu may be more common at certain times of the year only and there may be a sudden spurt in such claims during these seasons. It is important to account for such trends so that they do not appear as outliers in the data and the machine does not classify them as suspicious though they can be expected at that time of the year.

These inputs to the model are given by domain experts- doctors, medical experts, and forensic analysts to account for these factors. In addition, features to be inputted are selected concerning the context and how they are expected to drive the fraud in a logical flow to ensure that spurious causal relations are not established. Confounding factors should be accounted for and tests of multicollinearity should be applied to ensure that the model results are not biased. The data set is then divided into 2 parts- training data set for training the model and validation data for validating the results.

Post the data segmentation and feature selection, it is important to identify the appropriate AI /ML model(s) to use for the data set at hand. This requires econometrics/data science skills to understand the underlying distribution of the dependant and independent variables and the characteristics of the data to understand the particular modelling technique which would be most apt. For eg., Linear regressions assume the error terms are normally distributed and data is non-heteroskedastic, similarly logistic regression assumes the linearity of independent variables and log odds. Similar assumptions need to be validated and tested by the econometrician before the appropriate model is selected. Also, validation of the modelling results requires specialised medical experts who can check the results of the model by conducting medical audits.

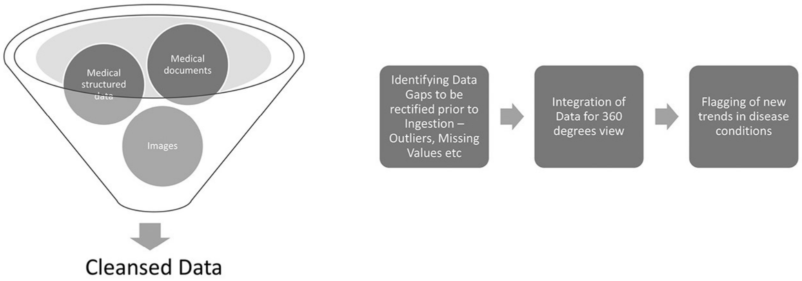
Medical structured data
Medical documents
Images
Cleansed Data
Identifying Data Gaps to be rectified prior to Ingestion – Outliers, Missing Values etc
Integration of Data for 360 degrees view
Flagging of new trends in disease conditions

Figure 1: Data Collection and Treatment

Data Analysis: An optimal approach for data analytics involves using semi-supervised models or a combination of both supervised learning and unsupervised learning. A multi-model approach enables better feature selection, removes 'noise' and significantly improves the accuracy of the results and helps take care of the limitations or biases which may be attributable to a specific technique. [57], [58]. Unsupervised learning techniques such as clustering can be used to classify the data followed by the development of supervised machine learning models such as logistic regression, decision trees etc. These 'non-black box' models allow the data scientist to look at the features being selected by the model as significant and the extent to which they influence the fraud score,

The results generated by the model can then be corroborated using deep learning techniques to compare the results of both models. The best model for each type of technique (supervised, unsupervised, deep learning) is finalised based on its performance on the validation data set. Claims which get classified as 'high risk' by at least one model are then sent for desk medical audit. The threshold of the risk level is set as per the volumes that can be analysed by the medical auditors. It is important to consider the specificity metric about the false-positive ratio in addition to the sensitivity metrics.

Medical audit of suspect claims: The audit process involves medical specialists who analyse the claims and the medical documents – diagnostic reports, and clinical notes to determine the necessity, quality of care and appropriateness of the treatment. In the first stage, the medical auditors analyse the suspect claims generated by the non-black-box models to understand the specific features (or their combination) which make the claim appear suspect. They may analyse the claim further and collect the appropriate evidence from the medical documents to confirm the case as genuine or fraudulent. For claims coming from neural network-based models, a two-stage process may be followed. In the first stage, the auditors analyse the medical documents to check if anything seems out of the pattern. If this is found to be the case, the specific elements of the medical documents help confirm the fraud and are then communicated to the fraud analyst who can then encode the specific data mining rules or encode them in the supervised learning algorithms. Most countries with strong public health insurance systems have invested in dedicated teams/organisations and the associated IT infrastructure to conduct desk and field audits of suspicious claims. In South Korea, the Health insurance Review and Assessment (HIRA) Service is responsible for reviewing claims and has strong systems in place to the augmentation of the human capacity for claims review [59]. Similarly, the Centre for Medicare and Medicaid (CMS), USA also has strong processes in place for audit of Medicare and Medicaid claims [60]. In all cases, adequate evidence must be collated before the denial of the claim. If further evidence is needed to post the desk medical audits, the suspect cases may also conduct surprise field visits to the hospital. Surprise visits also prevent the manipulation of documents by the provider. Post the field investigation, the final set of confirmed fraud transactions is shared back with the adjudicators, who can then reject the fraud claims and approve the genuine ones. It is also shared with analysts who use the final labelled data set for further fine-tuning of the model and training it. The final interpretation of outcomes is done by analytics and domain experts who recommend policy modifications to control the fraud. These could include the removal of certain errant providers from the network or requiring further documents to prove the medical necessity of the treatment [60]–[62].

Regular monitoring and updating of the model with new trends/findings: Given the dynamic nature of fraud, the performance of various models/ algorithms should be monitored regularly to ensure that low-performing models are refined or phased out. Any new patterns in fraud are identified immediately and should be inputted into the model to classify the suspicious claims. Further information on new types of disease conditions should also be fed into the model by the analysts. The models are constantly being trained with the inputs which come from the audit confirmation of cases as fraud/nonfraud. The entire process described above can be summarised in Figure 2.

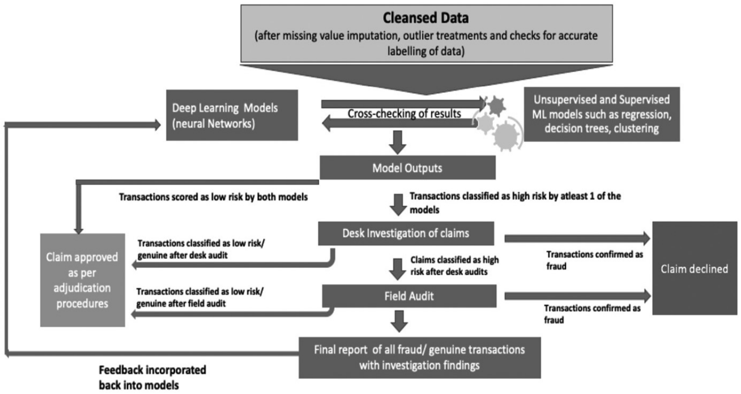
Cleansed Data
(after missing value imputation, outlier treatments and checks for accurate labelling of data)
Deep Learning Models (neural Networks)
Cross-checking of results
Unsupervised and Supervised ML models such as regression, decision trees, clustering
Model Outputs
Transactions scored as low risk by both models
Transactions classified as high risk by atleast 1 of the models
Desk Investigation of claims
Claim approved as per adjudication procedures
Transactions classified as low risk/ genuine after desk audit
Claims classified as high risk after desk audits
Transactions confirmed as fraud
Claim declined
Transactions classified as low risk/ genuine after field audit
Field Audit
Transactions confirmed as fraud
Final report of all fraud/ genuine transactions with investigation findings
Feedback incorporated back into models

Figure 2: Process flow under augmented AI/ML strategy for claims adjudication

Sample audits should be conducted on false positives and false negative cases to refine results. It is not very uncommon that certain specialists who are highly reputed in case of certain procedures, get a disproportionate volume of cases. This might make them appear aberrant compared to their peers. Similarly, certain tertiary care hospitals may be handling more complicated cases even for the same disease, such as patients with multiple morbidities etc. In that case, they may need to keep the patient admitted for a longer period, use branded medication and conduct diagnostic tests on a more frequent basis, which might make them appear to be indulging in waste or upcoding. It is important to recognise these differences and supplement the knowledge of the data with these inputs available from the local market sources. For this district-level officials should also have an important role not only in field investigations but also during the model-building process. Once a hospital has been identified as 'non-fraud' post audits and investigations, an appropriate override flag may be assigned to it for some 'cool-off' period to avoid auditing the hospital again and again for the same reason. This would ensure that providers do not get hassled by the process and help to ensure trust between the provider and payer. In case of claim denials, The reasons for the denial with the auditors' findings must be communicated clearly to the provider so that there is full transparency to the provider.

Conclusion:

The paper examined the use of AI/ML models in the area of health claims fraud detection, outlining the unique nuances of healthcare systems that make them particularly prone to fraud. We then looked at the key limitations of using siloed AI/ML models in health claims fraud detection. The paper then laid down a comprehensive hybrid approach for effective fraud control where the AI/ML algorithms can be supplemented with the human intelligence of the analyst to not only accurately classify the data for modelling purposes but also identify more contextual features and better prediction of fraud trends and take corrective action.

Given the sensitivities in the case of health claims adjudication, where an incorrect denial of a genuine claim can lead to treatment denials or adverse patient health outcomes, it becomes all the more important to leverage AI/ML augmentation of human decisions and not as their replacement. The process of how the fraud is suspected and confirmed also needs to be absolutely clear and transparent as these need to be explained to the provider. This requires a strong integration and confluence of the combined knowledge of humans as well as the speed and accuracy of AI/ML systems.

References

[1] GSMA, “State of Mobile Internet Connectivity Report-2020,” pp. 8–60, 2020.

[2] L. T. Khrais, “Role of artificial intelligence in shaping consumer demand in e-commerce,” *Future Internet*, vol. 12, no. 12, pp. 1–14, 2020, doi: 10.3390/fi12120226.

[3] V. A. Brei, “Machine learning in marketing,” *Foundations and Trends in Marketing*, vol. 14, no. 3, pp. 173–236, 2020, doi: 10.1561/1700000065.

[4] O. Arandjelovic, S. Stubseid, and O. A. Arandjelovi´c, “Machine Learning Based Prediction of Consumer Purchasing Decisions: The Evidence and Its Significance Surveillance,” *Workshops at the Thirty-Second AAAI …*, pp. 100–106, 2018.

[5] H. Shin, H. Park, J. Lee, and W. C. Jhee, “A scoring model to detect abusive billing patterns in health insurance claims,” *Expert Systems with Applications*, vol. 39, no. 8, pp. 7441–7450, 2012, doi: 10.1016/j.eswa.2012.01.105.

[6] H. He, J. Wang, W. Graco, and S. Hawkins, “Application of Neural Networks to Detection of Medical Fraud,” 1997.

[7] C. Francis, N. Pepper, and H. Strong, “Using support vector machines to detect medical fraud and abuse.,” *Conference proceedings : ... Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Conference*, pp. 8291–8294, 2011.

[8] T. Ekin, F. Leva, F. Ruggeri, and R. Soyer, “Application of bayesian methods in detection of healthcare fraud,” in *Chemical Engineering Transactions*, 2013, vol. 33, pp. 151–156. doi: 10.3303/CET1333026.

[9] Q. Liu and M. Vasarhelyi, “Healthcare fraud detection: A survey and a clustering model incorporating Geo-location information,” 2013.

[10] M. Kirlidog and C. Asuk, “A Fraud Detection Approach with Data Mining in Health Insurance,” *Procedia - Social and Behavioral Sciences*, vol. 62, pp. 989–994, 2012, doi: 10.1016/j.sbspro.2012.09.168.

[11] I. Kose, M. Gokturk, and K. Kilic, “An interactive machine-learning-based electronic fraud and abuse detection system in

healthcare insurance," *Applied Soft Computing Journal*, vol. 36, pp. 283–299, Aug. 2015, doi: 10.1016/j.asoc.2015.07.018.

[12] P. A. Ortega, C. J. Figueroa, and G. A. Ruz, "A Medical Claim Fraud/Abuse Detection System based on Data Mining: A Case Study in Chile," 2006.

[13] J. M. Johnson and T. M. Khoshgoftaar, "Medicare fraud detection using neural networks," *J Big Data*, vol. 6, no. 1, Dec. 2019, doi: 10.1186/s40537-019-0225-0.

[14] R. Y. Gupta, S. S. Mudigonda, and P. K. Baruah, "A comparative study of using various machine learning and deep learning-based fraud detection models for universal health coverage schemes," *International Journal of Engineering Trends and Technology*, vol. 69, no. 3, pp. 96–102, 2021, doi: 10.14445/22315381/IJETT-V69I3P216.

[15] C. Zhang, X. Xiao, and C. Wu, "Medical fraud and abuse detection system based on machine learning," *Int J Environ Res Public Health*, vol. 17, no. 19, pp. 1–11, 2020, doi: 10.3390/ijerph17197265.

[16] P. Babuna, X. Yang, A. Gyilbag, D. A. Awudi, D. Ngmenbelle, and D. Bian, "The impact of covid-19 on the insurance industry," *International Journal of Environmental Research and Public Health*, vol. 17, no. 16, pp. 1–14, 2020, doi: 10.3390/ijerph17165766.

[17] A. Bollmann *et al.*, "Utilization of in- And outpatient hospital care in Germany during the Covid-19 pandemic insights from the German-wide Helios hospital network," *PLoS ONE*, vol. 16, no. 3 March, pp. 1–7, 2021, doi: 10.1371/journal.pone.0249251.

[18] O. Smith, P. Naib, P. K. Sehgal, and S. Chhabra, "PM-JAY Under Lockdown: Evidence on Utilization Trends," *World Bank*, pp. 1–12, 2020.

[19] Transparency International, "Global Corruption Report 2006," 2006. doi: 10.2307/j.ctt184qq53.

[20] K. J. Arrow, "Uncertainty and the Welfare Economics of Medical Care," *American Economic Review*, vol. 53. pp. 941–696, 1963. doi: Article.

[21] K. Hussmann, "Addressing Corruption in the Health Sector: Securing Equitable Access to Health Care for Everyone," *U4 Issue*, no. 1, p. 39, 2011.

[22] W. D. Savedoff, “Transparency and Corruption in the Health Sector : A Conceptual Framework and Ideas for Action in Latin American and the Caribbean,” *Inter-American Development Bank*, vol. Note 3, no. May, pp. 1–29, 2007.

[23] M. Sparrow, “Fraud Control in the Health Care Industry: Assessing the State of the Art,” *National Institute of Justice Journal*, vol. JR000235, no. 1042, p. 11, 1998.

[24] D. Thornton, M. Brinkhuis, C. Amrit, and R. Aly, “Categorizing and Describing the Types of Fraud in Healthcare,” *Procedia Comput Sci*, vol. 64, no. December, pp. 713–720, 2015, doi: 10.1016/j.procs.2015.08.594.

[25] R. Gaitonde, A. D. Oxman, P. O. Okebukola, and G. Rada, “Interventions to reduce corruption in the health sector,” *Cochrane Database of Systematic Reviews*, vol. 2016, no. 8. John Wiley and Sons Ltd, Aug. 16, 2016. doi: 10.1002/14651858. CD008856.pub2.

[26] P. C. Dean, J. Vazquez-Gonzalez, and L. Fricker, “Causes and Challenges of Healthcare Fraud in the US,” *International Journal of Business and Social Science*, vol. 4, no. 14, p. 4, 2013.

[27] J. D. Byrd, P. Powell, and D. L. Smith, “Health care fraud: an introduction to a major cost issue,” *Journal of Accounting, Ethics & Public Policy Volume 14, No. 3*, 2013.

[28] J. H. Zhao, X. Li, and Z. Y. Dong, “Online Rare Events Detection,” in *Advances in Knowledge Discovery and Data Mining*, 2007, pp. 1114–1121.

[29] A. Carreño, I. Inza, and J. A. Lozano, “Analyzing rare event, anomaly, novelty and outlier detection terms under the supervised classification framework,” *Artificial Intelligence Review*, vol. 53, no. 5, pp. 3575–3594, 2020, doi: 10.1007/s10462-019-09771-y.

[30] S. S. Waghade, “A Comprehensive Study of Healthcare Fraud Detection based on Machine Learning,” 2018.

[31] E. Wanyonyi, A. Rodrigues, S. Abeka, and S. Ogara, “Effectiveness Of Security Controls On Electronic Health Records,” *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, vol. 6, 2017.

[32] H. Shin, H. Park, J. Lee, and W. C. Jhee, "A scoring model to detect abusive billing patterns in health insurance claims," *Expert Systems with Applications*, vol. 39, no. 8, pp. 7441–7450, Jun. 2012, doi: 10.1016/j.eswa.2012.01.105.

[33] J. R. Gaikwad, A. B. Deshmane, H. V Somavanshi, S. V Patil, and R. A. Badgujar, "Credit Card Fraud Detection using Decision Tree Induction Algorithm," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, no. 6, pp. 2278–3075, 2014.

[34] J. T. Hancock and T. M. Khoshgoftaar, "Gradient Boosted Decision Tree Algorithms for Medicare Fraud Detection," *SN Computer Science*, vol. 2, no. 4, pp. 1–12, 2021, doi: 10.1007/s42979-021-00655-z.

[35] H. He, J. Wang, W. Graco, and S. Hawkins, "Application of Neural Networks to Detection of Medical Fraud," 1997.

[36] U. Srinivasan and B. Arunasalam, "Leveraging big data analytics to reduce healthcare costs," *IT Prof*, vol. 15, no. 6, pp. 21–28, 2013, doi: 10.1109/MITP.2013.55.

[37] T. Vian, "Review of corruption in the health sector: Theory, methods and interventions," *Health Policy Plan*, vol. 23, no. 2, pp. 83–94, 2008, doi: 10.1093/heapol/czm048.

[38] S. P. Sood *et al.*, "Electronic medical records: A review comparing the challenges in developed and developing countries," *Proceedings of the Annual Hawaii International Conference on System Sciences*, no. November 2015, 2008, doi: 10.1109/HICSS.2008.141.

[39] G. Rieder and J. Simon, "Big Data: A New Empiricism and its Epistemic and Socio-Political Consequences," *Berechenbarkeit der Welt?*, pp. 85–105, 2017, doi: 10.1007/978-3-658-12153-2_4.

[40] J. Burrell, "How the machine 'thinks': Understanding opacity in machine learning algorithms," *Big Data and Society*, vol. 3, no. 1, pp. 1–12, 2016, doi: 10.1177/2053951715622512.

[41] M. T. Ribeiro, S. Singh, and C. Guestrin, "'Why should i trust you?' Explaining the predictions of any classifier," *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, vol. 13-17-Augu, pp. 1135–1144, 2016, doi: 10.1145/2939672.2939778.

[42] C. Chaix-Couturier, I. Durand-Zaleski, D. Jolly, and P. Durieux,

"Effects of financial incentives on medical practice: Results from a systematic review of the literature and methodological issues," *International Journal for Quality in Health Care*, vol. 12, no. 2, pp. 133–142, Apr. 2000, doi: 10.1093/intqhc/12.2.133.

[43] J. Clemens and J. D. Gottlieb, "Do physicians' financial incentives affect medical treatment and patient health?," *SIEPR Discussion Paper No. 11-017*, vol. 104, no. 4, pp. 1320–1349, 2012, doi: 10.1257/aer.104.4.1320.

[44] H. He, J. Wang, W. Graco, and S. Hawkins, "Application of Neural Networks to Detection of Medical Fraud," 1997.

[45] U. Office of the Inspector General, Department of Health and Human Services, "2020 National HealthCare Fraud Takedown. Accessed at https://oig.hhs.gov/newsroom/media-materials/2020takedown/ on 24th Jan 2022," 2020.

[46] Europäisches Parlament, *The ethics of artificial intelligence issues and initiatives : study Panel for the Future of Science and Technology*, no. March. 2020.

[47] V. Gawron, "Automation in Aviation — Accident Analaysis," *MITRE Technical Report*, no. 16, 2019.

[48] H. J. Wilson and P. R. Daugherty, "Collaborative Intelligence: Humans and AI Are Joining Forces. Accessed at https://hbr.org/2018/07/collaborative-intelligence-humans-and-ai-are-joining-forces on 18th Nov 2021," *Harvard Business Review July–August 2018*, 2018.

[49] OECD Centre for Responsible Business Conduct, "Artificial Intelligence and Responsible Business Conduct. Accessed at https://mneguidelines.oecd.org/RBC-and-artificial-intelligence.pdf on 19th Nov 2021," pp. 1–9, 2019.

[50] D. Wang *et al.*, "Human-AI collaboration in data science: Exploring data scientists' perceptions of automated AI," *Proc ACM Hum Comput Interact*, vol. 3, no. CSCW, 2019, doi: 10.1145/3359313.

[51] T. Kanakubo and H. Kharrazi, "Comparing the Trends of Electronic Health Record Adoption Among Hospitals of the United States and Japan," *Journal of Medical Systems*, vol. 43, no. 7, 2019, doi: 10.1007/s10916-019-1361-y.

[52] Y.-G. Kim *et al.*, “Rate of electronic health record adoption in South Korea: A nation-wide survey.,” *International journal of medical informatics*, vol. 101, pp. 100–107, May 2017, doi: 10.1016/j.ijmedinf.2017.02.009.

[53] M. Esdar, J. Hüsers, J.-P. Weiß, J. Rauch, and U. Hübner, “Diffusion dynamics of electronic health records: A longitudinal observational study comparing data from hospitals in Germany and the United States.,” *International journal of medical informatics*, vol. 131, p. 103952, Nov. 2019, doi: 10.1016/j.ijmedinf.2019.103952.

[54] J. Liang *et al.*, “Adoption of Electronic Health Records (EHRs) in China During the Past 10 Years: Consecutive Survey Data Analysis and Comparison of Sino-American Challenges and Experiences.,” *Journal of medical Internet research*, vol. 23, no. 2, p. e24813, Feb. 2021, doi: 10.2196/24813.

[55] Y. H. Su, C. P. Chao, L. C. Hung, S. F. Sung, and P. J. Lee, “A natural language processing approach to automated highlighting of new information in clinical notes,” *Applied Sciences (Switzerland)*, vol. 10, no. 8, 2020, doi: 10.3390/APP10082824.

[56] Y. Juhn and H. Liu, “Artificial intelligence approaches using natural language processing to advance EHR-based clinical research,” *Journal of Allergy and Clinical Immunology*, vol. 145, no. 2, pp. 463–469, 2020, doi: 10.1016/j.jaci.2019.12.897.

[57] K. Patel, S. M. Drucker, J. Fogarty, A. Kapoor, and D. S. Tan, “Using multiple models to understand data,” *IJCAI International Joint Conference on Artificial Intelligence*, pp. 1723–1728, 2011, doi: 10.5591/978-1-57735-516-8/IJCAI11-289.

[58] A. Bonarini, “A Multimodel Approach to Reasoning and Simulation,” *IEEE Transactions on Systems, Man and Cybernetics*, vol. 24, no. 10, pp. 1433–1449, 1994, doi: 10.1109/21.310527.

[59] Y. T. Park, J. S. Yoon, S. M. Speedie, H. Yoon, and J. Lee, “Health insurance claim review using information technologies,” *Healthcare Informatics Research*, vol. 18, no. 3, pp. 215–224, 2012, doi: 10.4258/hir.2012.18.3.215.

[60] Centre for Medicare and Medicaid, “MIP Medicaid Integrity Program National Medicaid Audit Program,” no. November, 2012.

[61] National Health Authority, “Ayushman Bharat PM-JAY Anti

Fraud Guidelines. Accessed at https://pmjay.gov.in/sites/default/files/2018-08/Anti-fraud-PMJAY-Guidelines.pdf on 22nd Sep 2021," 2018.

[62] GAO - U.S. Government Accountability Office, "A Framework for Managing Fraud Risks in Federal Programs," *International Journal of …*, no. July, p. 61, 2015.