A Review of Fraudulent Practices in Healthcare Insurance and Machine Learning-Based Investigation Approaches

Aishat Salau
Department of Computer Science
Nile University of Nigeria
Abuja, Nigeria
salauaishat@gmail.com

Prof. Nwojo Agwu Nnanna
Department of Computer Science
Nile University of Nigeria
Abuja, Nigeria
nagwu@nileuniversity.edu.ng

Prof. Moussa Mahamat Boukar
Department of Computer Science
Nile University of Nigeria
Abuja, Nigeria
musa.muhammed@nileuniversity.edu.ng

2023 14th International Conference on Information, Intelligence, Systems & Applications (IISA) | 979-8-3503-1806-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/IISA59645.2023.10345969

***Abstract*— Healthcare insurance fraud is a complex and costly problem that has become a concern globally. Traditional methods of detecting fraudulent claims and requests are time-consuming and often ineffective. Machine learning methods offer potential solutions to this problem by improving fraud investigation and prevention in health insurance systems. This paper presents a comprehensive review of machine learning-based approaches for addressing healthcare insurance fraud, as well as associated challenges and limitations. Despite limitations, our findings suggest that fraud could be effectively tackled by addressing the challenges identified. Areas for further research were also highlighted.**

Keywords*— Healthcare insurance fraud; fraud detection; machine learning; pre-authorization; healthcare insurance claims.

I. INTRODUCTION

Healthcare insurance fraud is prevalent globally and continues to be on the increase in the healthcare sector despite measures put in place to combat its widespread [1]. Its exponential rise continues to eat into governments' coffers. In the United States (US), up to 10% of 3.5 trillion dollars spent on healthcare is expended on waste, abuse and fraud with records indicating that this is predicted to rise every year [2, 3]. Also according to estimates from the United States Federal Bureau of Investigation (FBI), healthcare fraud costs US citizens between $70 and $234 billion each year [4]. In Romania, about 5% (up to €300 million) of the healthcare budget per year accounts for its expenditure on health insurance fraud [5]. Similarly, in South Africa, an estimated amount of ZAR13Billion is lost to fraudulent claims in the private health sector [6].

Fraud in health insurance is the intentional provision of false or misleading information to a health insurance company in an attempt to have them pay unauthorized benefits to a person or entity [1]. Although abuse and waste are not particularly related to fraud except when done deliberately. Abuse is when a provider's practices fall short of acceptable practices, leading to payment for services that are medically unnecessary, while the waste is the unnecessary provision and overuse of healthcare services [7].

Beyond wastage of healthcare resources and financial losses, fraud affects the quality of the healthcare system. To address this issue, it is essential to devise strategies that eliminate waste, abuse, and fraud. However, this requires an understanding of its various manifestations and the entities involved in the health insurance scheme, including the healthcare providers (HCP), health maintenance organizations (HMO), and enrollees (insurance subscribers) [8]–[10]. By comprehending the magnitude and nature of the problem, efforts can be directed towards effectively combating health insurance fraud.

Throughout the system, from the enrollee's visit to the healthcare provider (HCP) to the reimbursement of the HCP by the health maintenance organization (HMO), several processes are implemented to prevent fraud. These steps encompass preauthorization, verification of services rendered, and review of claims for reimbursement purposes [11]. When carried out manually, these processes turn out ineffective considering the millions of requests and claims that are submitted for review [12]. However, with the advancement of technology and need for increased efficiency, information systems based on data mining and machine learning methods have been employed to automate and simplify this processes [9, 13]. This paper is aimed at providing insights into the potential of machine learning as a tool for fraud prevention and detection in healthcare insurance, identifying methods and challenges in implementing these approaches in real-world settings, as well as highlighting directions for further research.

The rest of the paper is structured as follows: Section II presents related works and Section III presents health insurance fraud investigation approaches, including relevant works of literature based on machine learning. In Section IV, the findings of the survey and respective limitations are discussed, while the conclusion and suggestions for future studies are covered in Section V.

II. RELATED WORKS

A few reviews have been carried out on fraud detection in the area of healthcare. A systematic review was conducted in [14], on the relevance of the use of machine learning for fraud detection in healthcare. The review analyzed related articles from various sources, and highlights the need for innovative approaches, such as machine learning, to improve fraud detection in this domain. A detailed study of fraud detection in healthcare using machine learning techniques was also carried out in [10], emphasizing the various fraud categories and fraud detection methodologies. A review of data mining techniques for detecting health care fraud and abuse was conducted by [15] with focus on supervised and unsupervised data mining approaches. They noticed that most studies have concentrated on algorithmic data mining with little emphasis or applicability to fraud detection efforts in the context of health care delivery or health insurance policy. Likewise, [16] in his work reviewed proposed data mining techniques for fraud detection in health insurance with focus on classification and clustering methods, he also highlighted the source and type of healthcare data used. Furthermore, in [17], a systematic

979-8-3503-1806-7/23/$31.00 ©2023 IEEE

Authorized licensed use limited to: Wikipedia. Downloaded on January 20,2025 at 09:19:02 UTC from IEEE Xplore. Restrictions apply.

review of literature was carried out identifying the types and perpetrators of fraud as well as various methods of fraud detection in health services including administrative and technical approaches. Li et al in their work [13], also categorized health insurance fraud actors in addition to a survey of statistical methods used for fraud detection in health insurance. Another comprehensive survey carried out in [18] elaborated on health insurance fraud types based on the actors, reviewed healthcare insurance fraud detection methods based on supervised learning techniques, and highlighted relevant sources of medical fraud detection datasets that could be used with supervised learning methods. To the best of our knowledge, there has been no review that has considered examining the subject from a proactive and reactive perspective.

III. Healthcare Insurance Fraud Investigation using Machine Learning

In this section we present a taxonomy of the research area as seen in Fig. 1, and discuss the challenges with the use of machine learning for healthcare fraud insurance investigation.

A. Fraud Types

Healthcare fraud is a complex issue and to develop effective fraud detection systems, it is essential to understand the specific type and nature of fraud being committed. Researchers have classified various types of healthcare fraud based on the stakeholders involved in the scheme, as evidenced in existing literature [13, 18]. In this study, we classify fraud types into the following groups:

1) Service Frauds: Service fraud involves any attempt by stakeholders to exploit medical services. This could include:

- Provision of unnecessary services
- False diagnosis or treatment
- Misrepresenting non-covered treatments as medically necessary covered treatments for purposes of obtaining insurance payments.
- Prescription fraud, where HCPs prescribe unnecessary or excessive medications, or individuals obtaining prescriptions under false pretenses.
- Receiving kickbacks or other incentives for referring patients to certain services or providers, which can lead to unnecessary or inappropriate medical care.
- Wrongfully denying or delaying valid claims to try to discourage the enrollee, with hopes that the they eventually give up.

2) Billing Fraud: Billing fraud occurs when HCPs submit false claims to insurance companies or government healthcare programs. This can include the following:

- Billing for services not provided
- Double Billing
- Unbundling; where a HCP creates separate claims for services or supplies that should be grouped, making it seem like separate treatments; billing each step of a single procedure as if they were separate procedures.
- Upcoding of services and items, where the HCP bills for services or equipment that are more expensive than the actual ones provided to the client [8].

3) Identity Fraud: This occurs when an individual or organisation steals another entity's medical identity and uses it to obtain medical services or benefits.

4) False documentation: This type of fraud involves falsifying documents such as medical records, billing statements, and insurance claims to obtain undeserved payments or benefits. False documentation could be used to conceal other types of fraudulent activity.

5) Conspiracy fraud: This involves the participation of more than one stakeholder in fraudulent activities, for example; healthcare provider and patient, insurance company and healthcare provider etc.

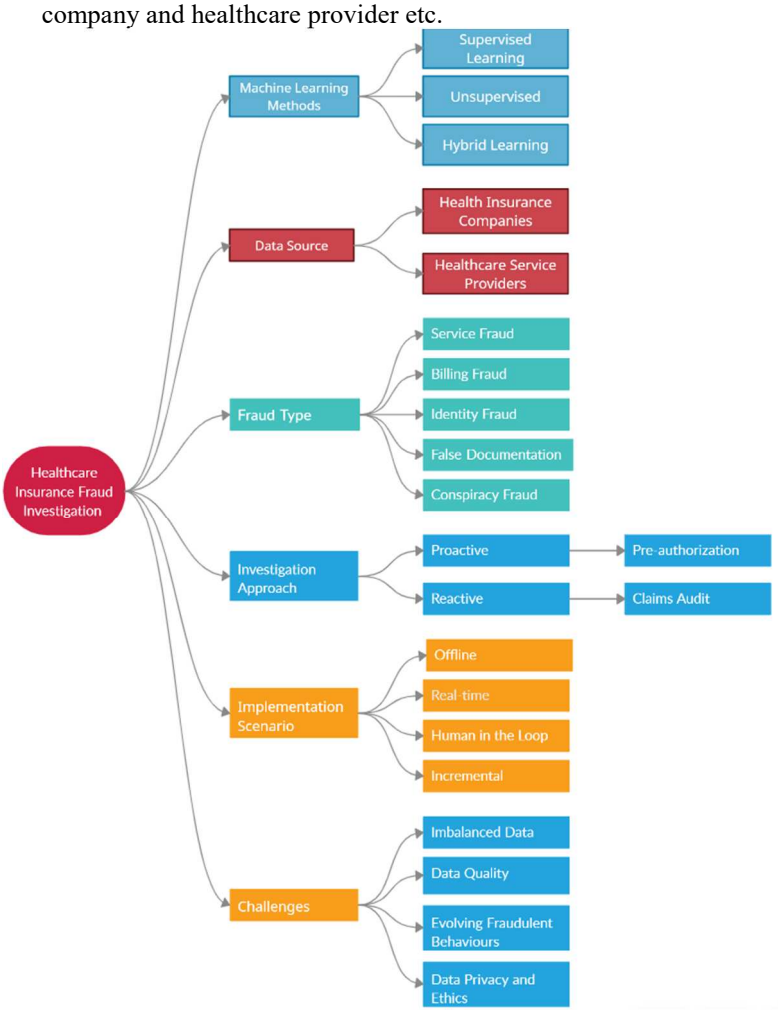

Fig. 1. Taxonomy of Healthcare Insurance Fraud Investigation

B. Fraud Investigation Approach

Fraud investigation approaches are methods employed to detect, investigate, and prevent fraud in the healthcare insurance industry. It can be classified broadly into proactive and reactive approaches. Proactive approaches involve implementing regulations, policies, procedures, staff training, compliance monitoring, and pre-authorization to prevent and help deter fraud before it happens. On the other hand, reactive approaches are responsive and involves reviewing claims data and identifying patterns of fraudulent behavior with the aim to minimize losses. This study emphasizes the utilization of machine learning to implement and enhance preauthorization and claims data review processes.

Authorized licensed use limited to: Wikipedia. Downloaded on January 20,2025 at 09:19:02 UTC from IEEE Xplore. Restrictions apply.

1) Pre-authorization

One of the known processes that has been implemented to prevent fraud, waste and abuse is pre-authorization [11]. The pre-authorization process necessitates healthcare providers to seek authorization from the HMO before certain services or medications are provided or rendered to patients. It is a method employed by the HMO to keep costs in check by eliminating error, waste, and unnecessary services. Besides cost-savings, pre-authorization is intended to enhance the quality of health care and ensure patients' safety [19].

The healthcare pre-authorization process is inefficient and labor-intensive, requiring constant manual review by multiple professionals [20]. To improve efficiency and reduce errors, researchers are exploring machine learning methods as a cost-effective solution [21]. Some of such proposals are seen in [11, 22, 23, 24].

2) Insurance Claims Review

HCPs submit claims to HMOs for reimbursements periodically. Traditionally, HMOs rely on a team of experienced medical professionals to review the large volume of healthcare claims submissions for discrepancies and fraudulent indications [10]. However, due to the exponential increase in the number of claims, this manual process becomes error-prone, time-consuming, expensive, and difficult to manage effectively [25]. Additionally, the evolving nature of fraud patterns complicate the task [26]. By leveraging machine learning algorithms, these approaches can be further enhanced to improve their accuracy, efficiency, and scalability.

C. Machine Learning Methods

Various machine learning techniques have been proposed by researchers in a bid to make the fraud investigation processes efficient; broadly classified into supervised, unsupervised and hybrid methods.

1) Supervised Learning

Supervised learning is a data mining technique used for prediction or classification tasks. It relies on labeled datasets, where a target variable is learned from a set of attributes [27]. In fraud detection, supervised learning methods are utilized to detect known patterns of fraud and abuse by classifying new observations into fraudulent or legitimate categories [15]. Examples of supervised learning techniques commonly applied in health insurance fraud detection include Decision Trees, Random Forest (RF), Logistic Regression (LR), Naive Bayes (NB), Support Vector Machines (SVM), and Neural Networks (NN).

In [28], multiple machine learning models including RF, NB, LR, Gradient Boosting, and Artificial Neural Network (ANN) were trained on Medicare claims data for fraud detection in medical billing. The analysis showed that RF, Gradient Boosting, and ANN outperformed other models. This finding was consistent with the results of Gushe et al in [9], where RF demonstrated better performance than LR in processing claims data.

In [22], a decision support mechanism was developed for pre-authorization using an ensemble of Random Tree (RT), NB, SVM, and Nearest Neighbor classifiers on dental request dataset, achieving an accuracy of approximately 96%. Additionally, Araujo proposed the use of decision tree and induction rules in [23], achieving ratings above 90%.

Textual features were introduced in [11] and [28] to enhance the pre-authorization learning process through the utilization of different techniques such as bag-of-words and TF-IDF for data representation. These approaches led to notable advancements in the classification performance in both studies.

As fraud datasets are intrinsically skewed, with the vast majority of transactions being legitimate and only a small percentage are fraudulent. This poses a challenge for machine learning algorithms which are not optimized to handle imbalanced datasets, resulting in bias towards the majority class and poor performance in detecting fraudulent cases. To address this issue, in [29], oversampling and undersampling techniques were employed to address class imbalance in an health insurance claims dataset. Five algorithms, including Decision Tree, RF, XGBoost, Gradient Boost, LightGBM, and a baseline Neural Network model, were evaluated. Under-sampled Neural Network model outperformed other models. Similarly, in [30] data-level and algorithmic-level techniques, including random over-sampling (ROS), random under-sampling (RUS), a hybrid approach combining ROS and RUS, and cost-sensitive loss functions like Focal Loss and Mean False Error loss, were explored.

Gradient Boosted Decision Trees (GBDT) are known to be well suited for heterogeneous data of which health insurance claims data is one of. In [31], the performance of three GBDT algorithms (XGBoost, CatBoost, and LightGBM) was evaluated on a fraud detection task using the Medicare Dataset [32]. CatBoost demonstrated superior performance compared to other classifiers, especially when handling categorical features.

Bauder et al, in [2], compared the performance of Train – Test and Cross-Validation (CV) evaluation methods and found that Train – Test performed better.

One of the limitations of traditional machine learning algorithms is their inability to scale on large dataset [33], while NNs are suited for large data. To leverage this advantage, Shamitha and Ilango in [34] proposed an optimized fraud detection framework for Medicare fraud detection built on a Multi-Layer Perceptron (MLP), optimized using genetic algorithm. This model performed better than traditional machine learning models. In another study conducted [35], MLP was also seen to perform best in a claims data review task, when evaluated alongside RF, SVM, Gradient Boosted Classifier and Adaboost algorithms.

Deep learning has been widely recognized for its superior performance in analyzing unstructured data, such as text data, outperforming other traditional machine learning methods. In [36], a two-layer deep neural network based on Long Short-Term Memory (LSTM) autoencoder was used to predict Medicare fraud using Medicare claims dataset. When compared with other state-of-art methods, it outperformed other classifiers. Similarly, deep learning algorithms were employed to detect fraud in claims data in [37], which resulted in a significant improvement in the claims management process compared to state-of-the-art models.

Supervised learning methods have been seen to show some acceptable performance and optimal accuracy in detecting known patterns of fraud and abuse [12]. Albeit,

Authorized licensed use limited to: Wikipedia. Downloaded on January 20,2025 at 09:19:02 UTC from IEEE Xplore. Restrictions apply.

with some shortcomings including the difficulties surrounding obtaining labeled healthcare data due to cost [38], change the pattern of claims, policies, thereby necessitating the need to regularly update training data sets of systems based on supervised learning methods [39]. Considering these shortcomings, unsupervised and hybrid learning techniques could serve as better alternatives [27].

2) Unsupervised Learning

In unsupervised learning, there are no target variables to predict or classify; instead, it segments samples into different groups by finding patterns in the dataset. This appears to be a promising technique given most publicly available healthcare datasets are unlabeled [27]. With these methods, potential fraudulent transactions just need to be identified and then experts determine the legitimacy of the transactions [40]. These are less costly and can detect new kinds of fraud as compared to supervised methods [41]. Some examples of unsupervised learning algorithms used in health insurance fraud detection include association rules, clustering algorithms, and outlier detection.

Outlier detection was applied to patients' dental data in [42], resulting in successful identification of fraudulent activities. Random Forest is a well-known prediction model but its use in unsupervised models is limited. In a comparative analysis [43], Unsupervised Random Forest was used amongst other outlier detection methods including, Isolation Forest, K-means Nearest Neighbor (KNN), Auto encoder and Local Outlier Factor (LOF) to detect fraud in Medicare claims data. LOF outperformed other algorithms. Similarly, in [44], Isolated Forest was found to produce favorable results compared to existing methods using K-means and Local Outlier Factor in detecting likely fraudulent healthcare providers. In [45], association scores were computed for three entities (patient, doctor, service), and G-means clustering was used over the scores to predict whether a case is a fraud or not. Lastly, [46] proposed an unsupervised multivariate analysis model to detect fraudulent behaviors in health insurance claims using a Weighted Multi-Tree and density-based clustering approach.

In health care fraud detection, most unsupervised methods have been combined with supervised methods. Although unsupervised learning eliminates the weaknesses associated with the inadequacy of labeled data in supervised learning, it is prone to wrong partitioning or segmentation of new data samples [27].

3) Hybrid Methods

These are a combination of different learning methods in order to enhance prediction or classification outcomes by leveraging the advantages of each method. These methods can also use a mix of labeled and unlabeled data. In [47], an approach to detect fraud in claims data by forming correlations and associations between claims attributes was proposed. This approach proposed Evolving Clustering method; association mining rule (to identify associated attributes and generate association rules) and SVM for classification of abuse or fraudulent claims. A novel fraud detection model was developed by hybridizing Genetic Algorithm and SVM [48]. The Genetic SVM (GSVM) showed reduced computation time in processing claims while achieving up to 87.91% accuracy. In [49], a hybrid framework combining rule engine, Decision Trees and Averaged Perceptron, outlier analysis, and k-means clustering techniques was used to identify fraudulent claims. In another study, a Heterogeneous Ensemble Model with Clustering is proposed for the effective detection of fraud in Medicare claims data [50]. The ensemble consists of MLP, LR, Cart and RF algorithms.

Hybrid methods could also be a combination of machine learning method and other technologies as seen in [51] and [52], where machine learning and blockchain technology are employed for fraud detection in healthcare. While machine learning algorithms is used to predict fraud, the blockchain technology provides a secure and tamper-proof way of storing and sharing data between different parties, ensuring immutability, traceability, and audit ability. The combination of these two technologies can lead to more accurate and efficient fraud detection in a secure and transparent manner.

Hybrid methods are considered to be the most effective approach for detecting fraud in health insurance [5]. This is because they can be used to eliminate the weaknesses associated with other learning methods and can leverage both labeled and unlabeled data, for better performance [27, 38].

Table 1 summarizes the recent literature on fraud detection using machine learning techniques, the source of the datasets used, evaluated algorithms, and results.

D. Implementation Scenarios

There are various scenarios in which the machine learning models for fraud investigation can be implemented, including offline, real-time, human in the loop, and incremental approaches.

Offline: In this scenario, the machine learning models are trained on a dataset that is collected beforehand. The trained model is then used to detect fraud in the health insurance system. Although this approach does not allow for real-time fraud detection, it can be effective in detecting fraud patterns that are well-established.

Real-time: This approach involves the detection of fraud in real-time as it occurs. This approach is beneficial for detecting new and emerging fraud patterns that may not have been captured in the training dataset. The use of real-time data streams allows for the early detection of fraud and a timely response. This approach can also be useful for applications where immediate action is required based on predictions.

Human-in-the-loop: This approach involves the collaboration between the machine learning model and a human expert. The machine learning model provides predictions, and the human expert validates the predictions. This approach is useful when there is uncertainty in the predictions made by the machine learning model or limited available data from model training. This scenario may require more time and resources to implement, but it can also provide greater accuracy and reliability.

Incremental: In this scenario, machine learning models are updated as new data becomes available, allowing the model to adapt to changes in the data over time. This approach is useful in addressing the ever-changing nature of the health insurance system.

The choice of implementation scenario will depend on factors such as the size and complexity of the data, the

Authorized licensed use limited to: Wikipedia. Downloaded on January 20,2025 at 09:19:02 UTC from IEEE Xplore. Restrictions apply.

desired level of accuracy, the resources available for implementation, and the specific needs and requirements of the application.

E. Challenges of Using Machine Learning in Fraud Investigation

While machine learning models have shown promise in detecting fraudulent records by learning sample characteristics or features, there are inherent challenges (most of which are data related) associated with using machine learning for fraud detection in health insurance systems [12, 53]. One major challenge is the issue of class imbalance, where the number of fraudulent cases is significantly smaller than the number of non-fraudulent cases. This can lead to biased models that prioritize accuracy on the majority class, while ignoring the minority class. Another challenge is the lack of labeled data for supervised learning. This is particularly problematic in healthcare, where fraud cases may be rare and difficult to identify. Unsupervised learning methods could help address this issue, but can also lead to high false positive rates with a risk of incorrect segmentation of data.

Additionally, the interpretability of machine learning models can be an issue in the healthcare sector, where transparency and accountability are critical. Another challenge is the constantly evolving nature of fraud tactics, which requires continuous updating and retraining of the models [39]. Similarly, the complexity and variability of healthcare data can make data preprocessing and feature engineering challenging. Finally, ethics and privacy are also a burning concern when using machine learning for fraud detection in healthcare.

TABLE I. AN SUMMARY OF LITERATURES ON MACHINE LEARNING TECHNIQUES FOR HEALTHCARE INSURANCE FRAUD

Publications	Algorithms	Dataset	Outcomes
Supervised Learning Methods			
[2]	LR, RF and GBT	Medicare Claims data	Test-train: GBT,AUC = 0.78281 Train-CV:LR, AUC = 0.74120
[9]	RF and LR	Medicare Claims data	RF performed better; ACC = 83.6%
[11]	RF, KNN and SVM	Brazilian HMO dataset	SVM and KNN performed best; Refused Class: P = 0.86, R = 1; Approved Class: P = 1, R = 0.98, K = 0.92
[22]	Random Tree, NB, SVM and Nearest Neighbor	Dental dataset from a non-profit health insurance company.	Ensemble (SVM, NN, RT) performed best P = 0.96, R = 0.98, ACC = 0.96, F1 = 0.96, AUC = 0.95, K = 0.94
[23]	Decision Tree and Induction Rules	Authorization requests from a nonprofit health insurance company Medical data	Classifier by Induction Rules showed better performance: Authorized Class: R = 97.07%, Unauthorized Class: R = 100%
[24]	NB, Sequential Minimal Optimization, Instance-based K, J48 and RF	Authorization data from a non-disclosed source	RT performed best with Refused Class: P = 0.872, R = 0.826 and F1 = 0.848 Approved Class: P = 0.835, R = 0.878 and F1 = 0.856
[28]	RF, NB, LR, GBT and ANN	Medicare Claims data	GBT performed best, P = 93.3%, R = 93.3%, AUC = 97%, F1 = 93%
[29]	Decision Tree, RF, XGBoost, GBT, LightGBM and NN	India health insurance data	NN + RUS performed best with F1-score = 0.95
[32]	GBDT, CatBoost, XGBoost and LightGBM	Medicare Claims data	CatBoost performed best; ACC = 99%, AUC = 0.7745
[34]	Optimized MLP	CMS Medicare data	ACC= 85.3%, P = 97% , R= 73%
[35]	RF, SVM, MLP, Adaboost, and GBT	Healthcare Providers fraud detection dataset from Kaggle repository	MLP performed best; ACC = 98%, AUC = 0.527, F1 = 88.9%
[36]	LSTM-based autoencoder	Medicare Claims data	AUC = 0.745, P = 0.770
Unsupervised Learning Methods			
[42]	Outlier Detection	US Medicaid dental claim data	71% accurately predicted dental providers for investigation
[43]	Unsupervised RF, Isolation Forest, KNN, Auto encoder and LOF	Medicare Claims data	LOF performed best; AUC = 0.6298
[44]	Isolated Forest, K-means and LOF	Medicare Dataset	ACC = 98.76%, AUC = 89.21%, F1 = 97.62%, P = 97%.
[45]	G-means clustering	Insurance claim data of a local hospital	Patient rating: 99-100 Service wrt patient rating: 98-100 Service wrt doctor rating: 98-100
[46]	Weighted Multi-Tree and density-based clustering	CMS Part B Program claims	ACC = 92%
Hybrid Methods			
[47]	Evolving Clustering method; association mining rule, and SVM	Health insurance claims data of Malaysian universities and insurance companies.	Proposed Theoretical Framework
[48]	Genetic Algorithm and SVM	Ghana National Health Insurances Subscribers' data	ACC = 87.91%
[49]	Rule engine, Decision Trees & Averaged Perceptron, outlier analysis, and K-means	Insirance claims	ACC = 0.946, AUC = 0.982, R = 0.968, F1 = 0.966.
[50]	Heterogeneous Ensemble Model with Clustering	Medicare insurance claims	ACC = 0.99, P = 0.96, R = 0.82, F1 = 0.88

ACC=Accuracy, P=Precision, R=Recall, F1=F1-score, AUC=Area Under ROC Curve

Authorized licensed use limited to: Wikipedia. Downloaded on January 20,2025 at 09:19:02 UTC from IEEE Xplore. Restrictions apply.

F. Data Sources

The primary sources of data for healthcare fraud investigation are HMOs (health insurance companies), either government or private, because they are often the payers of healthcare services and therefore have a financial incentive to detect and prevent fraudulent activities. Data can also be sourced from healthcare service providers. It is worth noting that most fraud insurance data made available for research are insurance claims, which limits the scope to reactive fraud investigation approaches. Also, while there are many publicly available claims datasets for research purposes, the same cannot be said for preauthorization datasets, which are currently nonexistent. This presents a significant disadvantage to researchers as limited access to data restricts their ability to test and validate their methods, limiting the potential for innovation and progress in proactive fraud investigation research efforts. Fig.2 depicts the number of research that use data from each major source.

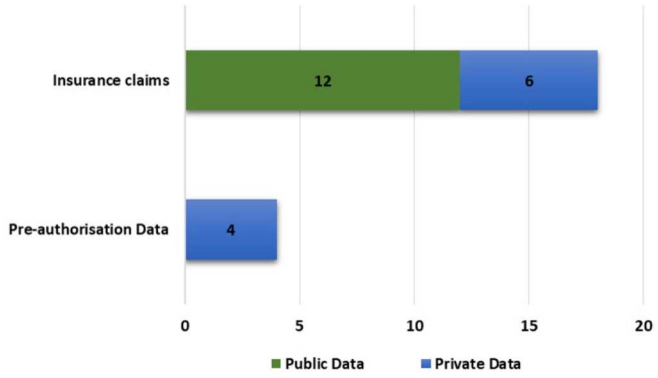

Fig. 2. Representation of Data Sources and Approach used in Reviewed Publications

G. Ethics and Privacy

Ethical principles must be at the forefront of decision-making frameworks in all areas of research and clinical practice, including the use of machine learning. As new technologies emerge, it is expected that new ethical dilemmas will arise [54]. The ethical principle of "Do No Harm" is essential, and a predictive ML algorithm must not be harmful at a minimum [55]. While the use of machine learning in fraud detection has the potential to save significant amounts of money and resources, it also raises ethical and privacy concerns. False positives are a major concern, which can lead to incorrect accusations and negatively impact individuals or healthcare providers' reputation. Moreover, there is a risk of bias in the data used to train machine learning models, which can lead to discrimination against certain groups. To ensure ethical and fair use of ML algorithms in fraud detection, it is necessary to consider algorithmic fairness and generalizability [56].

Furthermore, the use of personal health information (PHI) including personal and confidential information such as medical history, diagnoses, and treatments, in fraud investigation raises privacy concerns for patients, providers, and insurance companies alike, as there is a risk that this data could be leaked or misused, leading to breaches of privacy and violation of ethical codes. PHI is sensitive information that must be protected under the Health Insurance Portability and Accountability Act (HIPAA) and other privacy laws. Compliance to these laws is paramount ensuring that relevant data is adequately protected and de-identified data should be nearly impossible to re-identify. Various researches [57, 58, 59, 60, 61] highlight several privacy preserving techniques to address this challenge.

IV. Findings and Discussion

Machine learning techniques show promise for addressing fraud in the health insurance system. Various methods, from decision trees to deep learning, have been explored, with deep learning showing potential for higher accuracy. Different data sources, including claims data and pre-authorization requests, have been used for fraud detection. However, there are limitations in the reviewed literature as outlined next.

- Health insurance fraud is a significant issue that requires proactive measures. However, the majority of reviewed studies (82%) focused on predicting and detecting fraudulent activities in insurance claims data, while only a few addressed the identification of fraud, waste, and abuse through pre-authorization processes.
- Access to pre-authorization request data is limited, as evident in the percentage presented in this review. This limits researchers' ability to effectively test and validate methods using this valuable data source. Access to such data needs to be increased to enhance fraud prevention efforts.
- Healthcare data is highly dynamic in nature, and patterns of both legitimate and fraudulent activities can change over time. Hence, a fraud detection system must be equipped with self-learning and evolving capabilities to adapt to the changes. Future research should consider the use of incremental learning methods, which can enable machine learning models adapt and evolve as new data becomes available.
- The reviewed studies did not consider real-time fraud detection for pre-authorization. Implementing real-time fraud detection systems can improve effectiveness prevention by promptly identifying and addressing new fraud patterns.
- Healthcare data, being sensitive, are rarely accessible for research without ensuring privacy preservation. Researchers must prioritize de-identification and informed consent to protect patient privacy and comply with ethical and legal guidelines, mitigating the risk of data breaches.
- The representation of clinical text data and its semantics into formats that can be used by ML algorithms have been a major challenge in the healthcare domain [62], and few works in this domain have considered this. Findings shows that using textual representation can improve performance of ML models. Word embeddings are vector-based representations of words, with the ability to encode syntactic and semantic word relationships accurately [63, 64]. This can hence be explored in future research for better representation of data and performance of ML models.
- Over half of the reviewed studies proposed the use of conventional machine learning algorithms, with

Authorized licensed use limited to: Wikipedia. Downloaded on January 20,2025 at 09:19:02 UTC from IEEE Xplore. Restrictions apply.

neural network-based algorithms showing superior performance compared to traditional approaches in [29] and [35]. Further exploration of deep learning methods could be beneficial in addressing fraud in health insurance.

- Despite the improved performance, the black-box nature of these deep learning algorithms make it difficult to understand how a decision was made, which can be problematic from an ethical standpoint. The lack of interpretability can also make it challenging to identify and correct errors or biases in the model, which could inadvertently limit their employability in real-world setting where transparency and accountability is not negligible.
- Literature also reveals that there are very few studies from underdeveloped and developing countries even though they are more susceptible and liable to this occurrence and its consequences [26].

Despite these limitations, the findings of this review suggest that machine learning methods have the potential to significantly improve fraud investigation and prevention in the health insurance system. By addressing the challenges identified and implementing the recommendations outlined, researchers and practitioners can develop more effective and efficient fraud prevention and detection systems that can help improve the quality of healthcare and save cost.

V. Conclusion and Future studies

In conclusion, this review aimed to address the increasing cases of fraud in healthcare systems and the resulting negative impact on patients in need of medical care. By exploring the application of machine learning methods for fraud investigation in health insurance, a taxonomy of the research area and associated challenges were provided. The potential for deep learning methods in this field was also highlighted. The review recommends further research in the area of preauthorization, application of deep learning, real-time data, active learning, and incremental learning for fraud prevention and investigation. Additionally, the development of explainable ML for healthcare insurance should be considered.

References

[1] W. L. Shiau, K. Siau, Y. Yu, and J. Guo, "Research Commentary on IS/IT Role in Emergency and Pandemic Management: Current and Future Research," *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/JDM.2021040105*, vol. 32, no. 2, pp. 67–75, Jan. 2021, doi: 10.4018/JDM.2021040105.

[2] R. A. Bauder, M. Herland, and T. M. Khoshgoftaar, "Evaluating model predictive performance: A medicare fraud detection case study," in *Proceedings - 2019 IEEE 20th International Conference on Information Reuse and Integration for Data Science, IRI 2019*, Jul. 2019, pp. 9–14, doi: 10.1109/IRI.2019.00016.

[3] "CMS Office of the Actuary releases 2017-2026 Projections of National Health Expenditures | CMS." https://www.cms.gov/newsroom/press-releases/cms-office-actuary-releases-2017-2026-projections-national-health-expenditures (accessed May 12, 2020).

[4] N. National Health Care Anti-Fraud Association, "Combating Health Care Fraud in a Post-Reform World : Seven Guiding Principles for Policymakers A White Paper Presented by The National Health Care Anti-Fraud Association," 2010.

[5] A.-R. Bologa, R. Bologa, and A. Florea, "Big Data and Specific Analysis Methods for Insurance Fraud Detection," *Database Syst. J.*, vol. I, pp. 30–38, 2010.

[6] T. G. Legotlo and A. Mutezo, "Understanding the types of fraud in claims to South African medical schemes," *South African Med. J.*, vol. 108, no. 4, p. 299, Mar. 2018, doi: 10.7196/samj.2017.v108i4.12758.

[7] J. Bush, L. Sandridge, C. Treadway, K. Vance, and A. C. D. Ph, "Medicare fraud, waste and abuse," *undefined*. 2017.

[8] D. Thornton, M. Brinkhuis, C. Amrit, and R. Aly, "Categorizing and Describing the Types of Fraud in Healthcare," in *Procedia Computer Science*, Jan. 2015, vol. 64, pp. 713–720, doi: 10.1016/j.procs.2015.08.594.

[9] N. Ghuse, P. Pawar, and A. Potgantwar, "An Improved Approch For Fraud Detection In Health Insurance Using Data Mining Techniques," 2017.

[10] S. S. Waghade, "A Comprehensive Study of Healthcare Fraud Detection based on Machine Learning," 2018.

[11] K. Farias, P. Santos Neto, A. Santana, and R. Bezerra Neto, "Using historical information of patients for prior authorization learning," in *Proceedings - 2019 Brazilian Conference on Intelligent Systems, BRACIS 2019*, Oct. 2019, pp. 598–603, doi: 10.1109/BRACIS.2019.00110.

[12] 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, Oct. 2020, doi: 10.3390/ijerph17197265.

[13] J. Li, K. Y. Huang, J. Jin, and J. Shi, "A survey on statistical methods for health care fraud detection," *Health Care Management Science*, vol. 11, no. 3. pp. 275–287, Sep. 2008, doi: 10.1007/s10729-007-9045-4.

[14] R. Ikono, O. Iroju, J. Olaleke, and T. Oyegoke, "Meta-analysis of fraud, waste and abuse detection methods in healthcare," *Niger. J. Technol.*, vol. 38, no. 2, p. 490, Apr. 2019, doi: 10.4314/njt.v38i2.28.

[15] H. Joudaki *et al.*, "Using data mining to detect health care fraud and abuse: a review of literature," *Global journal of health science*, vol. 7, no. 1. Canadian Center of Science and Education, pp. 194–202, Jan. 01, 2015, doi: 10.5539/gjhs.v7n1p194.

[16] M. P. Pawar, "Review on Data Mining Techniques for Fraud Detection in Health Insurance," *Int. J. Emerg. Trends Technol.*, vol. 3, no. 2, pp. 1128–1131, Jul. 2016.

[17] A. Y. B. R. Thaifur, M. A. Maidin, A. I. Sidin, and A. Razak, "How to detect healthcare fraud? 'A systematic review,'" *Gac. Sanit.*, vol. 35, pp. S441–S449, Jan. 2021, doi: 10.1016/J.GACETA.2021.07.022.

[18] P. Dua and S. Bais, "Supervised learning methods for fraud detection in healthcare insurance," *Intell. Syst. Ref. Libr.*, vol. 56, pp. 261–285, 2014, doi: 10.1007/978-3-642-40017-9_12.

[19] "Considerations for Improving Prior Authorization in Healthcare," 2019.

[20] [20] A. Medical Association, "2019 AMA prior authorization (PA) physician survey," 2019.

[21] Caqh, "2018 CAQH INDEX ® A Report of Healthcare Industry Adoption of Electronic Business Transactions and Cost Savings," doi: 10.1001/jama.2018.1150.

[22] F. H. D. Araújo, A. M. Santana, and P. de A. Santos Neto, "Using machine learning to support healthcare professionals in making preauthorisation decisions," *Int. J. Med. Inform.*, vol. 94, pp. 1–7, Oct. 2016, doi: 10.1016/j.ijmedinf.2016.06.007.

[23] F. Araújo, L. Moraes, A. Santana, P. S. Neto, P. Adeodato, and É. Leão, "Evaluation of the use of computational intelligence techniques in medical claim processes of a health insurance company," in *Proceedings of CBMS 2013 - 26th IEEE International Symposium on Computer-Based Medical Systems*, 2013, pp. 23–28, doi: 10.1109/CBMS.2013.6627759.

[24] G. V. M. Junior, J. P. A. Vieira, R. L. De Sales Santos, J. L. N. Barbosa, P. De Alcantara Dos Santos Neto, and R. S. Moura, "A study of the influence of textual features in learning medical prior authorization," in *Proceedings - IEEE Symposium on Computer-Based Medical Systems*, Jun. 2019, vol. 2019-June, pp. 56–61, doi: 10.1109/CBMS.2019.00021.

[25] 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, pp. 224–231.

[26] A. Rashidian, H. Joudaki, and T. Vian, "No evidence of the effect of the interventions to combat health care fraud and abuse: A

Authorized licensed use limited to: Wikipedia. Downloaded on January 20,2025 at 09:19:02 UTC from IEEE Xplore. Restrictions apply.

systematic review of literature," *PLoS ONE*, vol. 7, no. 8. Aug. 24, 2012, doi: 10.1371/journal.pone.0041988.

[27] R. Bauder, T. M. Khoshgoftaar, and N. Seliya, "A survey on the state of healthcare upcoding fraud analysis and detection," *Heal. Serv. Outcomes Res. Methodol.*, vol. 17, no. 1, pp. 31–55, Mar. 2017, doi: 10.1007/s10742-016-0154-8.

[28] N. Obodoekwe and D. T. van der Haar, "A Comparison of Machine Learning Methods Applicable to Healthcare Claims Fraud Detection," in *Advances in Intelligent Systems and Computing*, Feb. 2019, vol. 918, pp. 548–557, doi: 10.1007/978-3-030-11890-7_53.

[29] R. Yashraj Gupta, P. Kumar Baruah, and S. Sai Mudigonda, "A Comparative Study of Using Various Machine Learning and Deep Learning-Based Fraud Detection Models For Universal Health Coverage Schemes," *Int. J. Eng. Trends Technol.*, vol. 69, pp. 96–102, 2021, doi: 10.14445/22315381/IJETT-V69I3P216.

[30] J. M. Johnson and T. M. Khoshgoftaar, "Medicare fraud detection using neural networks," vol. 6, p. 63, 2019, doi: 10.1186/s40537-019-0225-0.

[31] L. Prokhorenkova, G. Gusev, A. Vorobev, A. V. Dorogush, and A. Gulin, "CatBoost: unbiased boosting with categorical features," *proceedings.neurips.cc*.

[32] J. T. Hancock and T. M. Khoshgoftaar, "Gradient Boosted Decision Tree Algorithms for Medicare Fraud Detection," *SN Comput. Sci.*, vol. 2, no. 4, Jul. 2021, doi: 10.1007/S42979-021-00655-Z.

[33] H. S. R. Rajula, G. Verlato, M. Manchia, N. Antonucci, and V. Fanos, "Comparison of Conventional Statistical Methods with Machine Learning in Medicine: Diagnosis, Drug Development, and Treatment," *Medicina (B. Aires).*, vol. 56, no. 9, pp. 1–10, Sep. 2020, doi: 10.3390/MEDICINA56090455.

[34] S. K. Shamitha and V. Ilango, "A time-efficient model for detecting fraudulent health insurance claims using Artificial neural networks," *2020 Int. Conf. Syst. Comput. Autom. Networking, ICSCAN 2020*, Jul. 2020, doi: 10.1109/ICSCAN49426.2020.9262298.

[35] S. Lavanya, S. Manojkumar, and M. Kumar, "Machine Learning Based Approaches for Healthcare Fraud Detection: A Comparative Analysis," *Ann. Rom. Soc. Cell Biol.*, vol. 25, no. 3, pp. 8644–8654, 2021.

[36] M. Zoubeirou, A. Mayaki, and M. Riveill, "Multiple Inputs Neural Networks for Medicare fraud Detection," Mar. 2022, doi: 10.48550/arxiv.2203.05842.

[37] I. Fursov *et al.*, "Sequence Embeddings Help Detect Insurance Fraud," *IEEE Access*, vol. 10, pp. 32060–32074, 2022, doi: 10.1109/ACCESS.2022.3149480.

[38] A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," *Journal of Network and Computer Applications*, vol. 68. Academic Press, pp. 90–113, Jun. 01, 2016, doi: 10.1016/j.jnca.2016.04.007.

[39] H. Cyrus, B. M. Affan, and S. A. Mehran, "A Review of Machine Learning Methods Applicable to Quality Issues," Mar. 2021, pp. 1225–1240.

[40] J. Copeland, L., Edberg, D., and Wendel, "Applying Business Intelligence Concepts to Medicaid Claim Fraud Detection," *J. Inf. Syst. Appl. Res.*, vol. 5, no. 1, pp. 51–61, 2012.

[41] T. Ekin, F. Ieva, F. Ruggeri, and R. Soyer, "Statistical issues in medical fraud assessment", Modelling and Scientific Computing," Milano, 2013.

[42] D. Thornton, G. Van Capelleveen, M. Poel, J. Van Hillegersberg, and R. M. Mueller, "Outlier-based health insurance fraud detection for U.S. medicaid data," in *ICEIS 2014 - Proceedings of the 16th International Conference on Enterprise Information Systems*, 2014, vol. 2, pp. 684–694, doi: 10.5220/0004986106840694.

[43] R. A. Bauder, R. C. Da Rosa, and T. M. Khoshgoftaar, "Identifying medicare provider fraud with unsupervised machine learning," in *Proceedings - 2018 IEEE 19th International Conference on Information Reuse and Integration for Data Science, IRI 2018*, Aug. 2018, pp. 285–292, doi: 10.1109/IRI.2018.00051.

[44] Kanksha, A. Bhaskar, S. Pande, R. Malik, and A. Khamparia, "An intelligent unsupervised technique for fraud detection in health care systems," *Intell. Decis. Technol.*, vol. 15, no. 1, pp. 127–139, 2021, doi: 10.3233/IDT-200052.

[45] I. Matloob, S. Khan, H. ur Rahman, and F. Hussain, "Medical health benefit management system for real-time notification of fraud using historical medical records," *Appl. Sci.*, vol. 10, no. 15, Aug. 2020, doi: 10.3390/app10155144.

[46] L. Settipalli and G. R. Gangadharan, "WMTDBC: An unsupervised multivariate analysis model for fraud detection in health insurance claims," *Expert Syst. Appl.*, vol. 215, p. 119259, Apr. 2023, doi: 10.1016/J.ESWA.2022.119259.

[47] S. Kareem, R. B. Ahmad, and A. B. Sarlan, "Framework for the identification of fraudulent health insurance claims using association rule mining," in *2017 IEEE Conference on Big Data and Analytics, ICBDA 2017*, Feb. 2018, vol. 2018-Janua, pp. 99–104, doi: 10.1109/ICBDAA.2017.8284114.

[48] R. Sowah, M. Kuuboore, A. Ofoli, … S. K.-J. of, and undefined 2019, "Decision Support System (DSS) for Fraud Detection in Health Insurance Claims Using Genetic Support Vector Machines (GSVMs)," *hindawi.com*.

[49] N. Rayan, "Framework for analysis and detection of fraud in health insurance," *Proc. 2019 6th IEEE Int. Conf. Cloud Comput. Intell. Syst. CCIS 2019*, pp. 47–56, Dec. 2019, doi: 10.1109/CCIS48116.2019.9073700.

[50] S. S. Kotekani and V. Ilango, "HEMClust: An Improved Fraud Detection Model for Health Insurance using Heterogeneous Ensemble and K-prototype Clustering," *IJACSA) Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 3, p. 2022.

[51] G. Zhang, X. Zhang, M. Bilal, W. Dou, X. Xu, and J. J. P. C. Rodrigues, "Identifying fraud in medical insurance based on blockchain and deep learning," *Futur. Gener. Comput. Syst.*, vol. 130, pp. 140–154, May 2022, doi: 10.1016/J.FUTURE.2021.12.006.

[52] B. K. Sethi, P. K. Sarangi, and A. S. Aashrith, "Medical Insurance Fraud Detection Based on Block Chain and Machine Learning Approach," pp. 1–4, Mar. 2023, doi: 10.1109/ICERECT56837.2022.10060811.

[53] N. R. Prasad, S. Almanza-Garcia, and T. T. Lu, "Anomaly detection," *Comput. Mater. Contin.*, vol. 14, no. 1, pp. 1–22, 2009, doi: 10.1145/1541880.1541882.

[54] T. Mathiesen and M. Broekman, "Machine Learning and Ethics," *Acta Neurochir. Suppl.*, vol. 134, pp. 251–256, 2022, doi: 10.1007/978-3-030-85292-4_28.

[55] K. K.-J. of clinical neuroscience and undefined 2019, "Medical ethics considerations on artificial intelligence," *Elsevier*, 2019, doi: 10.1016/j.jocn.2019.03.001.

[56] R. R. Fletcher, A. Nakeshimana, and O. Olubeko, "Addressing Fairness, Bias, and Appropriate Use of Artificial Intelligence and Machine Learning in Global Health," *Front. Artif. Intell.*, vol. 3, Apr. 2021, doi: 10.3389/FRAI.2020.561802/FULL.

[57] N. Khalid, A. Qayyum, M. Bilal, A. Al-Fuqaha, and J. Qadir, "Privacy-preserving artificial intelligence in healthcare: Techniques and applications," *Comput. Biol. Med.*, vol. 158, p. 106848, May 2023, doi: 10.1016/J.COMPBIOMED.2023.106848.

[58] K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, "Big healthcare data: preserving security and privacy," *J. Big Data*, vol. 5, no. 1, Dec. 2018, doi: 10.1186/S40537-017-0110-7.

[59] H. C. Tanuwidjaja, R. Choi, and K. Kim, "A Survey on Deep Learning Techniques for Privacy-Preserving," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11806 LNCS, pp. 29–46, 2019, doi: 10.1007/978-3-030-30619-9_4.

[60] P. Churi, & A. P.-J. of E. S., and undefined 2019, "A Systematic Review on Privacy Preserving Data Publishing Techniques.," *researchgate.net*, vol. 12, no. 6, pp. 17–25, 2019, doi: 10.25103/jestr.126.03.

[61] R. Torkzadehmahani *et al.*, "Privacy-Preserving Artificial Intelligence Techniques in Biomedicine," *Methods Inf. Med.*, vol. 61, pp. E12–E27, Jun. 2022, doi: 10.1055/S-0041-1740630.

[62] F. K. Khattak, S. Jeblee, C. Pou-Prom, M. Abdalla, C. Meaney, and F. Rudzicz, "A survey of word embeddings for clinical text," *J. Biomed. Inform.*, vol. 100, p. 100057, Jan. 2019, doi: 10.1016/J.YJBINX.2019.100057.

[63] P. D. Turney and P. Pantel, "From Frequency to Meaning: Vector Space Models of Semantics," 2010.

[64] Y. Wang *et al.*, "A comparison of word embeddings for the biomedical natural language processing," *J. Biomed. Inform.*, vol. 87, pp. 12–20, Nov. 2018, doi: 10.1016/j.jbi.2018.09.008.

Authorized licensed use limited to: Wikipedia. Downloaded on January 20,2025 at 09:19:02 UTC from IEEE Xplore. Restrictions apply.