THE ASEAN JOURNAL OF MILITARY AND PREVENTIVE MEDICINE

ISSN (e): 3031-870X
Vol. 3 No.2 (2026)
https://journal.ajmpm.net/

DOI: https://doi.org/10.47353/ajmpm.v3i2.72

Artificial Intelligence for Healthcare Fraud Prevention: A Systematic Literature Review

Ridwan[1], Dian Arlianty[2]

[1]Department of Accounting, Faculty of Economics and Business, Syiah Kuala University, Province Aceh, Banda Aceh, Indonesia
[2] Department of Biology Education, Faculty of Teacher Training and Education, Malikussaleh University, North Aceh, Indonesia

Email: *ridwan63@mhs.usk.ac.id*

Abstract

Background: Healthcare fraud threatens the sustainability, efficiency, and integrity of healthcare systems worldwide. Conventional fraud detection approaches are increasingly inadequate because of the growing complexity and volume of healthcare claims data. This study aimed to systematically review the application of artificial intelligence (AI) methods for healthcare fraud detection and to summarize current evidence on their potential contributions to fraud prevention.
Methods: A systematic literature review was conducted following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. Articles were retrieved from the Scopus database using the keywords "artificial intelligence" and "healthcare fraud". Studies were selected according to predefined inclusion and exclusion criteria, and twelve eligible studies were included in the qualitative synthesis.
Results: The reviewed studies suggest that supervised, unsupervised, and hybrid machine learning methods have the potential to support healthcare fraud detection. Frequently reported machine learning methods include Random Forest, Logistic Regression, Neural Networks, Bayesian models, CatBoost, and Isolation Forest, while blockchain was identified as a supporting technology for enhancing data integrity and security in healthcare fraud prevention. However, the effectiveness of these approaches depends on data quality, appropriate model validation, and continuous human oversight.
Conclusion: Current evidence suggests that artificial intelligence has considerable potential to strengthen healthcare fraud detection and support fraud prevention activities. Rather than replacing professional auditors, AI should be implemented as a decision-support tool integrated with robust governance, audit procedures, and human validation to enhance the transparency, efficiency, and sustainability of healthcare financing systems.
Keywords: *Artificial Intelligence; Healthcare Fraud; Machine Learning; Systematic Literature Review*

Background

Healthcare fraud remains a major challenge to the efficiency, sustainability, and integrity of healthcare systems.[1] Developing an efficient healthcare service system requires an effective way to detect fraud.[2] This research aims to examine the systematic literature on the use of artificial intelligence in detecting fraud occurring in healthcare services. Healthcare service costs in Indonesia have continued to rise since the National Health Insurance (JKN) era in 2014 until 2021; this increase is influenced by the number of participants, healthcare service costs, and new technologies.[3] However, based on the findings of the government's internal auditor, the BPKP (Financial and Development Supervisory Agency), in 2018, there were findings of fraud in the JKN program regarding healthcare services, although the amount was 1% of the healthcare service costs paid. The iceberg phenomenon can occur with unidentified potential for fraud.[4] The data indicates opportunities for various stakeholders in fraudulent activities. Therefore, innovation in artificial intelligence systems is needed to reduce the level of fraud in healthcare services.

Fraud arises from insufficient oversight; the larger the funds managed, the greater the potential for fraud.[5] High fraud can hinder the organization's sustainability.[6] There is a need to strengthen adequate policies and systems because fraud is difficult to detect or measure. Fraud is a form of intentional deception that occurs during an event that falls under the category of crime or moral hazard.[7] Fraud can be committed by stakeholders such as participants, healthcare providers, and insurance personnel.[8] Fraud perpetrators are predominantly internal, such as employees, and in this case, in healthcare services, one of them is from the medical profession, with cases of fictitious claims. When acting, perpetrators tend not to be alone but rather within a systemic and networked organization. The appropriate method for detecting healthcare fraud is through secondary data tracking, information, and the provision of technological applications.[9]

These conditions and situations make it difficult for policymakers, anti-fraud professionals, and practitioners to find reliable evidence and keep up with the literature published in various formats and different references. Sufficient audit evidence is based on the assessment of misstatements, and as an example, the audit relevance evidence collected.[10] Audit evidence will be required if it has a low level of risk and relevance, and vice versa. Artificial intelligence is a field of study that uses intelligent thinking to create more controlled computing systems, making it easier for users to analyze a problem or document.[11] Therefore, artificial intelligence has audit characteristics; that is, it is sufficient to meet the requirements of auditing standards. The computer system's ability to interpret healthcare data can be processed and interpreted more consistently in accordance with regulatory requirements.

AI-based algorithmic decision-making has the potential to strengthen healthcare fraud prevention. The influence of algorithm-based decision-making on fraud potential can improve the quality of audit services.[12] A study conducted in Chile reported, in which a data mining–based fraud detection system identified approximately 75 cases of healthcare fraud and abuse per month, enabling detection approximately 6.6 months earlier than conventional approaches. Koreff et al. (2021) provided empirical evidence that data analytics can strengthen healthcare fraud auditing by supporting more effective identification of suspicious claims and improving audit decision-making. Othman et al. (2015) found that technological advancements have diminished proactive detection techniques that analyze data and transactions to isolate symptoms such as trends, figures, and other related anomalies. Fraud prevention and detection are appropriate protection mechanisms against fraud.[5]

Professional service between the patient as the principal and the doctor as the agent. Patients and doctors have different goals: patients want to be healthy while paying as little as possible, whereas doctors are interested in maximizing their income and therefore face the temptation to provide more medical services than necessary or charge higher prices than justified. In this case, the patient is disadvantaged because they cannot directly evaluate the service provided by the doctor. In short, there is information asymmetrically benefiting the doctor. The principal attempts to manipulate and shape the agent's behavior so that they will act in a manner consistent with the principal's preferences.[15]

Fraud prevention can be achieved by implementing policies related to the use of artificial intelligence in the health social security system or health insurance. There is extensive research on fraud occurring in healthcare services. However, there remains limited evidence regarding the application of artificial intelligence for healthcare fraud prevention. A systematic literature review has been published in various formats and different references. Therefore, a systematic literature review is crucial to provide useful information and reliable evidence for healthcare services regarding literature on fraud prevention.

Methods

This study employed a systematic literature review (SLR) approach and followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines to identify, select, and synthesize evidence regarding the application of artificial intelligence (AI) in healthcare fraud detection and prevention.

Literature Search Strategy

A systematic literature search was conducted in the Scopus database on 15 January 2023 using the following reproducible Boolean search strategy: TITLE-ABS-KEY (("artificial intelligence" OR "machine learning" OR "deep learning" OR "neural network") AND ("healthcare fraud" OR "medical fraud" OR "health insurance fraud"))

The search covered studies published from 2010 to 2022. The filters applied were English language, open-access publications, and eligible peer-reviewed publication types. Because this review included both journal articles and conference proceedings, the Scopus filters should be specified as follows: The search was limited to English-language, open-access publications indexed in Scopus. Eligible publication types included peer-reviewed journal articles and conference proceedings published between 2010 and 2022. The search was conducted in the Title, Abstract, and Keywords fields. The complete search string, database, filters, and search date were documented to ensure that the literature search could be reproduced.

Eligibility Criteria

Studies were selected using predefined inclusion and exclusion criteria. The inclusion criteria were: (1) peer-reviewed journal articles or peer-reviewed conference proceedings indexed in Scopus; (2) studies published in English between 2010 and 2022; (3) studies examining the application of artificial intelligence, machine learning, deep learning, neural networks, data mining, or related computational approaches to healthcare fraud detection or prevention; (4) studies addressing healthcare claims, medical fraud, health insurance fraud, healthcare-provider fraud, or related anomalous claim patterns; and (5) studies with accessible full text and sufficient information for data extraction.

The exclusion criteria were: (1) duplicate records; (2) conference abstracts without full papers, editorials, letters, commentaries, review protocols, theses, dissertations, and non-peer-reviewed publications; (3) studies unrelated to healthcare fraud; (4) studies that did not apply or evaluate an AI-related method; (5) studies without accessible full text; and (6) studies that did not provide sufficient methodological or empirical information relevant to the objectives of the review.

Data Extraction
Data were extracted using a standardized data-extraction form to ensure consistency across the included studies. The extracted information comprised author names, publication year, country, publication type, study design, dataset characteristics, AI or computational method, learning type, fraud-detection approach, validation method, performance measure, and principal findings.

The learning approaches were classified as supervised, unsupervised, or hybrid. Blockchain was classified separately as a supporting technology rather than as a machine-learning method.

Data Synthesis
The included studies differed substantially in their datasets, fraud definitions, AI algorithms, validation procedures, sampling methods, and performance metrics. Therefore, a meta-analysis was not considered appropriate. The findings were synthesized using a descriptive qualitative approach.

The synthesis focused on the types of AI methods used, their learning classifications, reported applications, approaches to class imbalance, validation procedures, methodological limitations, and potential contributions to healthcare fraud detection. Direct claims of superiority among algorithms were avoided because the reviewed studies used heterogeneous datasets and evaluation methods.

Study Selection
The study selection process followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines. A systematic literature search identified 172 records from the Scopus database using the predefined Boolean search strategy. No duplicate records or additional records were removed before screening. Therefore, all 172 records proceeded to title and abstract screening. During this stage, 19 records were excluded because they were not relevant to healthcare fraud detection, did not investigate artificial intelligence or machine learning applications, or did not meet the predefined eligibility criteria. Consequently, 153 reports were sought for retrieval, of which 7 reports could not be retrieved because the full text was unavailable.

Subsequently, 146 full-text reports were assessed for eligibility based on the predefined inclusion and exclusion criteria. During the full-text eligibility assessment, 134 studies were excluded for the following reasons: 73 studies were outside the scope of the review, 32 studies provided insufficient methodological detail, 12 studies did not report relevant empirical findings, and 17 studies were excluded for other reasons. These other reasons included studies that provided insufficient descriptions of the artificial intelligence methods, had unclear research objectives, focused on healthcare analytics rather than fraud detection, reported incomplete outcome measures, or did not provide sufficient information for data extraction and qualitative synthesis. Ultimately, 12 studies met all eligibility criteria and were included in the final qualitative synthesis. The complete study selection process is presented in **Figure 1.**

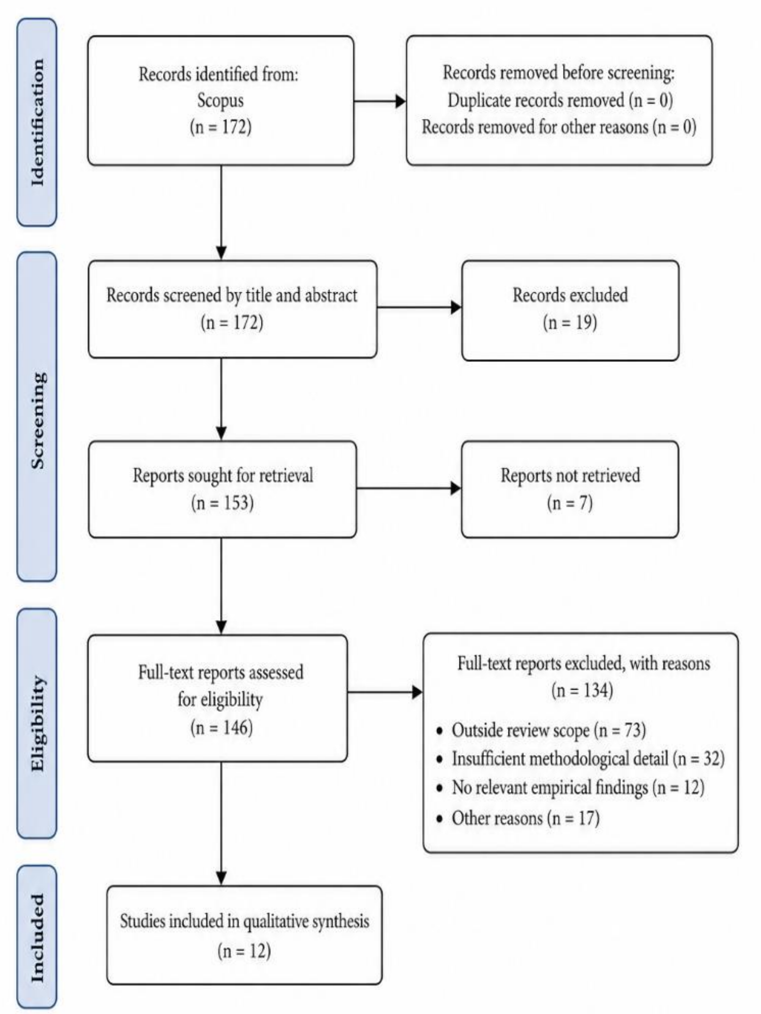

Figure 1. PRISMA 2020 flow diagram of the study selection process.

Results

The findings in this literature review identified 12 articles discussing the detection of healthcare fraud using artificial intelligence applications. A summary of the data extracted from the selected studies is presented in Table 1.

Table 1. Research on approach preventing Fraud in Healthcare

Author	AI Method	Learning Type	Main Findings
Ekin et al. (2013)	Bayesian Co-clustering	Supervised	Bayesian models effectively identify unusual provider–beneficiary relationships to support healthcare fraud audits.
Dua & Bais (2014)	Pattern Analysis	Supervised	Supervised machine learning effectively detects complex healthcare insurance fraud patterns.
Kose et al. (2015)	AHP + EM Clustering	Unsupervised	Interactive ML framework improves fraud detection efficiency through clustering and visualization.
Rawte (2015)	ECM + SVM	Hybrid	Combining supervised and unsupervised learning improves fraudulent claim detection.
Herland et al. (2018)	Logistic Regression, Random Forest, Gradient Tree Boosting	Supervised	Logistic Regression showed promising performance (AUC=0.816).
Bauder & Khoshgoftaar (2017)	Machine Learning Models	Hybrid	Supervised methods demonstrated promising performance within the evaluated Medicare dataset.
Johnson & Khoshgoftaar (2019)	Neural Network	Supervised	Neural networks effectively detected Medicare fraud, especially under class imbalance.
Bauder & Khoshgoftaar (2018)	Random Forest	Supervised	Random Forest demonstrated promising performance after addressing class imbalance.
Hancock & Khoshgoftaar (2020)	CatBoost	Supervised	CatBoost demonstrated promising performance within the evaluated Medicare dataset.
Zhang et al. (2020)	Neural Network	Supervised	Neural network improved anomaly detection and reduced analysts' workload.
Saldamli et al. (2020)	Blockchain	Supporting Technology	Blockchain enhances data integrity and security for healthcare fraud prevention; it is not a machine learning algorithm.
Kanksha et al. (2021)	Isolation Forest	Unsupervised	Isolation Forest demonstrated promising performance in the evaluated study.

Discussion

Machine learning applies statistical algorithms to data to uncover hidden patterns and make predictions about the future. [16] These tools can be broadly characterized as supervised, unsupervised, and hybrid. Based on the table above, the detection of anomalous data in healthcare services can utilize machine learning applications, which can be divided into three categories: supervised learning, unsupervised learning, and hybrid learning. There are 7 articles using a supervised approach, 2 unsupervised articles, 2 articles using both or a hybrid approach and 1 article supporting technology. Supervised methods use well-understood and labeled datasets to create models that can be applied prospectively. The guided learning application algorithms used for anomaly detection include coclustering, pattern analysis, Random Forest (RF), Gradient Tree Boosting (GTB), Logistic Regression (LR), Neural Networks (random over-sampling (ROS), random under-sampling (RUS), and a hybrid ROS–RUS), Random Forest with Class Imbalanced Big Data, neural network, and Blockchain.[2,17–23] The reviewed evidence suggests that supervised learning methods can perform well when reliable labeled datasets are available; however, their performance remains highly dependent on dataset characteristics and validation strategies. In addition, direct comparisons between these approaches remain limited because the reviewed studies employed different datasets, fraud definitions, outcome measures, and validation strategies. Furthermore, supervised learning algorithms are highly dependent on the dataset.[24] To prevent health insurance fraud, it is necessary to build a system to securely manage and monitor insurance activities by integrating data from all insurance companies. Because blockchain provides immutable data maintenance and sharing, we propose a blockchain-based solution for health insurance fraud detection.[23]

Unsupervised methods theoretically need to prove the consistency problem of outliers and anomalies. Unsupervised methods, on the other hand, are used to explore unlabeled data structures. When considering healthcare claims data, researchers face the challenge that, because not all cases of fraud are identified, the labeling applied to historical claims data cannot be considered completely accurate. In addition, unsupervised methods like clustering empower investigators to uncover and identify suspicious patterns in submitted claims that require further investigation. Previously, the investigation relied on the use of descriptive statistics to identify claim patterns that were several standard deviations above average in terms of the number of services performed or the costs submitted. Advanced clustering methods can reveal much more subtle deviations from normal practice patterns that were previously undetected. Literature analyzes methods such as analytic hierarchical processing (AHP), expectation maximization (EM), and the isolated forest algorithm.[25,26] Local outlier anomalies were studied and it was found that some of the data anomalies were caused by direct or indirect abuse or fraudulent behavior, proving the feasibility of outlier detection in detecting abnormal health insurance behavior. Unsupervised learning methods may provide valuable support for identifying previously unknown anomalies in healthcare claims and may complement supervised learning approaches when labeled data are limited. Outlier detection methods work by finding normative patterns in claims data and flagging instances that deviate. For example, healthcare facilities whose billing codes fall outside their normal scope of practice could become targets for auditors if such usage is not seen among a significant number of their peers. Another type of practice that might be flagged involves the use of codes that vary based on the number of services performed in a single visit; this behavior could be flagged as an anomaly compared to other healthcare facilities. Even if this specific incident wasn't the trigger for the audit, deviating from standard practices could result in future payments being subject to closer scrutiny. Therefore, it is important to properly document any practices that require deviation from standard practices whenever possible.

Data mining, which is divided into two learning techniques, supervised and unsupervised, is used to detect fraudulent claims. However, since each of the above techniques has its own advantages and disadvantages, by combining the strengths of both techniques, a new hybrid approach is proposed for detecting fraudulent claims in the health insurance industry.[18] Evolving Clustering Method (ECM), Support Vector Machine (SVM), Machine Learning Methods, and CatBoost.[18,22,27]

AI Limitations and Data Quality

Despite the promising performance of artificial intelligence in healthcare fraud detection, several limitations should be considered. The effectiveness of AI models depends heavily on the quality, completeness, consistency, and representativeness of healthcare claims data. Supervised models require correctly labeled historical data, whereas many fraudulent claims remain undetected or are confirmed only after further audit and investigation. Consequently, incomplete or inaccurate labels may reduce model sensitivity and limit its generalizability across healthcare systems.[19,24] In addition, variations in provider characteristics, claim structures, and fraud patterns can affect model performance, indicating that an algorithm developed using one dataset may not produce comparable results when applied to another population.[22,25] AI models must therefore be periodically validated, recalibrated, and retrained to address changing claim patterns and emerging fraud schemes.[20,26]

Class Imbalance in Healthcare Fraud Detection
Class imbalance is another major challenge because fraudulent claims generally represent only a small proportion of all healthcare claims. Under highly imbalanced conditions, machine learning algorithms may achieve high overall accuracy by classifying most records as legitimate while failing to identify the minority fraud class. Bauder and Khoshgoftaar demonstrated that model performance varied considerably according to the class distribution and sampling strategy used, and that a balanced 50:50 distribution did not necessarily produce the best detection results.[20] Johnson and Khoshgoftaar similarly examined random over-sampling, random under-sampling, and hybrid sampling approaches to improve neural-network performance in Medicare fraud detection.[20] Comparative evidence also indicates that supervised, unsupervised, and hybrid methods are affected differently by class imbalance and provider type.[24] Therefore, fraud-detection studies should evaluate sensitivity, specificity, precision, recall, F1-score, and the area under the receiver operating characteristic curve rather than relying only on overall accuracy.[19,22,27]

Human Validation and Auditor Oversight
Artificial intelligence should be regarded as a decision-support mechanism rather than a replacement for professional auditors and healthcare fraud investigators. AI-based models can identify unusual provider–beneficiary relationships, detect anomalous claim patterns, and prioritize high-risk cases for further examination; however, algorithmic alerts do not independently establish that fraud has occurred.[2,25] Human validation remains necessary to examine clinical justification, supporting documents, regulatory requirements, and the context underlying anomalous claims. The integration of data from different healthcare sources can strengthen the identification of suspicious transactions, but the resulting alerts must still be followed by audit procedures and investigation.[19,23] Auditor oversight is also essential for addressing false-positive results, ensuring accountability, and preventing inappropriate decisions based solely on automated outputs.[2,25]

Overall Interpretation and Future Direction
The reviewed evidence suggests that supervised learning methods are particularly useful when sufficiently reliable labeled data are available, while unsupervised methods can identify previously unknown anomalies within unlabeled claims data.[24,25,26] Hybrid approaches may combine the strengths of classification and anomaly detection, particularly when healthcare fraud labels are incomplete.[18,24] CatBoost, Random Forest, Logistic Regression, Neural Networks, and Isolation Forest showed promising performance across different datasets, although direct comparison remains difficult because the studies employed different samples, outcome measures, and validation procedures.[19,20,21,22,26,27] Future studies should therefore prioritize external validation, explainable AI, appropriate management of class imbalance, and continuous collaboration between data scientists, auditors, clinicians, and fraud investigators.

Overall, the reviewed evidence indicates that artificial intelligence offers promising opportunities to support healthcare fraud detection through a range of supervised, unsupervised, and hybrid machine learning approaches. However, the findings should be interpreted with caution because the included studies differed substantially in their datasets, fraud definitions, validation procedures, and performance metrics. Consequently, no single AI approach can be considered universally superior based on the current evidence. Future studies should emphasize explainable AI, rigorous external validation, and collaboration between AI systems and human experts to enhance the reliability, transparency, and practical implementation of healthcare fraud detection systems.

Conclusion

The findings of this systematic literature review suggest that artificial intelligence has considerable potential to improve healthcare fraud detection and support fraud prevention activities. Supervised, unsupervised, and hybrid machine learning approaches can assist healthcare organizations by identifying suspicious claim patterns and supporting fraud detection processes. Furthermore, the successful implementation of these approaches depends on high-quality healthcare data, appropriate model validation, continuous updating to accommodate evolving fraud patterns, and ongoing human oversight.

Although AI has the potential to support healthcare fraud detection, it should be regarded as a decision-support tool rather than a replacement for professional auditors. Final fraud determination requires audit procedures, investigation, and human judgment to verify AI-generated alerts and minimize false-positive results. Therefore, integrating AI-based technologies with robust governance, standardized audit procedures, and human oversight offers a promising strategy for strengthening healthcare fraud detection systems.

For healthcare systems such as Indonesia's National Health Insurance (JKN), the reviewed evidence indicates that adopting AI-based fraud detection technologies may enhance the effectiveness of claim monitoring and risk identification. Nevertheless, successful implementation requires adequate data quality, institutional readiness, regulatory support, and collaboration between data scientists, healthcare providers, and auditors to ensure transparent, accountable, and sustainable fraud prevention.

Acknowledgments

None.

Author Contributions

RR & DA conceived and designed the study, conducted the literature search and screening, analyzed and interpreted the data, drafted and critically revised the manuscript, and approved the final version for publication. The authors are responsible for the integrity and accuracy of all aspects of the work.

Conflict of Interest

None.

References

1. Sunarti S, Ghozali MT, Haris F, Rahman FF, Rahman RA, Ghozali. Preventing fraud and deficit through the optimization of health insurance in Indonesia. *Systematic Reviews in Pharmacy*. 2020;11(7):228-231. doi:10.31838/srp.2020.7.36

2. Ekin T, Leva F, Ruggeri F, Soyer R. Application of bayesian methods in detection of healthcare fraud. *Chem Eng Trans*. 2013;33:151-156. doi:10.3303/CET1333026

3. Agustina R, Dartanto T, Sitompul R, et al. Universal health coverage in Indonesia: concept, progress, and challenges. *The Lancet*. 2019;393(10166):75-102. doi:10.1016/S0140-6736(18)31647-7

4. Fatimah R, Misnaniarti M, Syakurah R. Potential Fraud in The Implementation of National Health Insurance in The Health Sector: Systematic Review. *Jurnal Medicoeticolegal dan Manajemen Rumah Sakit*. 2021;10(December):255-270. 10.18196/jmmr.v10i3.10825

5. Abdallah A, Maarof MA, Zainal A. Fraud detection system: A survey. *Journal of Network and Computer Applications*. 2016;68:90-113. doi:10.1016/j.jnca.2016.04.007

6. Rodgers W, Söderbom A, Guiral A. Corporate Social Responsibility Enhanced Control Systems Reducing the Likelihood of Fraud. *Journal of Business Ethics*. 2015;131(4):871-882. doi:10.1007/s10551-014-2152-5

7. Litton R. Moral hazard and insurance fraud. *Eur J Crim Pol Res*. 1995;3(1):30-47. doi:10.1007/BF02243131

8. Eldayana S, Wardiyah A, Samino. Hubungan Insentif Dana Kapitasi Jaminan Kesehatan Nasional (JKN) dengan Motivasi Kerja Pegawai Puskesmas Metro Tahun 2014. *Jurnal Kesehatan Holistik*. 2015;9(2):64-70.

9. Thaifur AYBR, Maidin MA, Sidin AI, Razak A. How to detect healthcare fraud? "A systematic review." *Gac Sanit*. 2021;35:S441-S449. doi:10.1016/j.gaceta.2021.07.022

10. Ryman-Tubb NF, Krause P, Garn W. How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Eng Appl Artif Intell*. 2018;76(July):130-157. doi:10.1016/j.engappai.2018.07.008

11. Joudaki H, Rashidian A, Minaei-Bidgoli B, et al. Using data mining to detect health care fraud and abuse: a review of literature. *Glob J Health Sci*. 2015;7(1):194-202. doi:10.5539/gjhs.v7n1p194

12. Ortega PA, Ruz GA, Figueroa CJ. A Medical Claim Fraud / Abuse Detection System based on Data Mining: A Case Study in Chile. *Proceedings of DMIN 2006*. 2006. doi:10.1.1.176.796

13. Koreff J, Weisner M, Sutton SG. Data analytics (AB) use in healthcare fraud audits. *International Journal of Accounting Information Systems*. 2021;42(June):100523. doi:10.1016/j.accinf.2021.100523

14. Othman R, Aris NA, Mardziyah A, Zainan N, Amin NM. Fraud Detection and Prevention Methods in the Malaysian Public Sector: Accountants' and Internal Auditors' Perceptions. *Procedia Economics and Finance*. 2015;28(April):59-67. doi:10.1016/s2212-5671(15)01082-5

15. Waterman RW, Meier KJ. Principal-Agent Models : An Expansion ? 1998;8:173-202.

16. Gordon D, Siegel DM. Machine learning and the future of Medicare fraud detection. *J Am Acad Dermatol*. 2020;83(2):e133. doi:10.1016/j.jaad.2020.03.059

17. Dua P, Bais S. Supervised learning methods for fraud detection in healthcare insurance. *Intelligent Systems Reference Library*. 2014;56:261-285. doi:10.1007/978-3-642-40017-9_12

18. Rawte V, Anuradha G. Fraud detection in health insurance using data mining techniques. *In: Proceedings of the 2015 International Conference on Communication, Information & Computing Technology (ICCICT);* 2015 Jan 16–17; Mumbai, India. p. 1–5. doi:10.1109/ICCICT.2015.7045689.

19. Herland M, Khoshgoftaar TM, Bauder RA. Big Data fraud detection using multiple medicare data sources. *J Big Data*. 2018;5(1):1-21. doi:10.1186/s40537-018-0138-3

20. Johnson JM, Khoshgoftaar TM. Medicare fraud detection using neural networks. *J Big Data.* 2019;6:63. doi:10.1186/s40537-019-0225-0.

21. Zhang C, Xiao X, Wu C. Medical fraud and abuse detection system based on machine learning. *Int J Environ Res Public Health*. 2020;17(19):1-11. doi:10.3390/ijerph17197265

22. Bauder RA, Khoshgoftaar TM. Medicare fraud detection using random forest with class imbalanced big data. *In: Proceedings of the 2018 IEEE 19th International Conference on Information Reuse and Integration for Data Science (IRI);* 2018 Jul 30–Aug 1; Salt Lake City, UT, USA. Piscataway (NJ): IEEE; 2018. p. 80–87. doi:10.1109/IRI.2018.00019.

23. Saldamli G, Reddy V, Bojja SK, Gururaja KM, Diddaveerappa Y, Tawalbeh L. Health insurance fraud detection using blockchain. *In: Proceedings of the 2020 7th International Conference on Software Defined Systems (SDS);* 2020 Apr 20–23; Paris, France. Piscataway (NJ): IEEE; 2020. p. 145–152. doi:10.1109/SDS49854.2020.9143892.

24. Bauder RA, Khoshgoftaar TM. Medicare fraud detection using machine learning methods. *In: Proceedings of the 16th IEEE International Conference on Machine Learning and Applications (ICMLA);* 2017 Dec 18–21; Cancun, Mexico. Piscataway (NJ): IEEE; 2017. p. 858–865.doi:10.1109/ICMLA.2017.00-48.

25. Kose I, Gokturk M, Kilic K. An interactive machine-learning-based electronic fraud and abuse detection system in healthcare insurance. *Applied Soft Computing Journal*. 2015;36:283-299. doi:10.1016/j.asoc.2015.07.018

26. Kanksha, Bhaskar A, Pande S, Malik R, Khamparia A. An intelligent unsupervised technique for fraud detection in health care systems. *Intelligent Decision Technologies*. 2021;15(1):127-139. doi:10.3233/IDT-200052

27. Hancock J, Khoshgoftaar TM. Medicare fraud detection using CatBoost. *In: Proceedings of the 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI)*; 2020 Aug 11–13; Las Vegas, NV, USA. Piscataway (NJ): IEEE; 2020. p. 97–103. doi:10.1109/IRI49571.2020.00022.