ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP1089

# Leveraging AI Algorithms to Combat Financial Fraud in the United States Healthcare Sector

Pelumi Oladokun [1],
Department of computer science
Southeast Missouri State University
Cape Girardeau, Missouri, USA

Adekoya Yetunde [2]
D'Amore-McKim School of Business
Northeastern University
Boston, MA, USA.

Temidayo Osinaike [3]
College of Information Assurance
St Cloud state University
Minnesota, USA.

Ikenna Obika [4]
College of Information Assurance
St Cloud state University
Minnesota, USA.

**Abstract:- Financial fraud is a major problem in the healthcare industry because it causes large financial losses and compromises the integrity and trust of healthcare systems. The intricacy and sophistication of contemporary fraudulent operations make conventional fraud detection techniques which rely on manual audits and rule-based systems increasingly inadequate. AI algorithms have become a viable way to improve financial fraud detection and prevention. Hence, this paper examines how AI algorithms can be used to detect and stop fraud in the healthcare industry, emphasizing how these algorithms could revolutionize fraud control procedures. This study suggests that AI algorithms greatly improve the identification of financial fraud in the healthcare industry by spotting intricate patterns and abnormalities frequently overlooked by already existing techniques. Machine learning models have proven to be highly accurate in predicting fraudulent claims and transactions. However, while AI provides numerous opportunities to improve fraud detection skills, its effective application necessitates resolving important issues, including ethical considerations, data governance, and model interpretability.**

***Keywords:-*** *Fraudulent Practices, Healthcare, Artificial Intelligence, Algorithms, Finance.*

## I. INTRODUCTION

The healthcare sector is essential to protect the health and welfare of individuals and communities. Fraud in the healthcare sector is a complicated issue involving various dishonest strategies to obtain unfair advantages from healthcare organizations. Most of these dishonest methods include unbundling (paying for products that should be bundled separately), upcoding (charging for a more expensive service than is delivered), billing for services that haven't been provided, and kickbacks [1]. The healthcare industry is therefore susceptible to financial fraud, which can lead to dire outcomes for patients, healthcare professionals, and the overall healthcare system.

Financial fraud in the healthcare sector pertains to dishonest practices that entail the misappropriation, manipulation, or falsification of financial resources in healthcare establishments or services. This kind of fraud in the healthcare industry is widespread in the United States, endangering patient care, resulting in large financial losses, and undermining public confidence in healthcare institutions. The report by [2] revealed that the United States loses tens of billions of dollars a year due to healthcare fraud. The United States healthcare system is especially prone to fraud because of its size, complexity, and complicated invoicing and payment procedures.

In the healthcare sector, AI is being used more and more to improve patient outcomes, optimize operational efficiency, and strengthen financial decision-making. AI facilitates the immediate detection of fraudulent activity by processing big datasets much faster and more precisely than humans [3; 4]. The use of AI in fraud detection is not without challenges, despite these benefits. Major challenges to widespread adoption include concerns about data privacy, algorithmic bias, the interpretability of AI models, and the necessity of integrating AI with the current healthcare IT infrastructure [5].

Furthermore, the quality and diversity of the data used to train these models which can differ throughout healthcare providers and institutions may also have an impact on the efficacy of AI-driven fraud detection systems [6]. It is imperative to detect and address financial fraud in the healthcare sector so as to protect the legitimacy, efficacy, and resilience of healthcare systems in the United States and globally. The purpose of this review is to summarize current information about the application of AI algorithms for

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP1089

healthcare fraud detection, to highlight best practices, and indicate areas that require further investigation.

## II. ROLE OF AI IN FINANCIAL FRAUD DETECTION

AI has established a new benchmark for fraud identification and prevention in the financial services departments of a variety of organizations, by demonstrating astounding efficacy in spotting irregularities. The efficacy of AI is attributed to its capacity to examine extensive datasets, identify complex patterns, and adjust to changing threats. Ha et al. [7] stated that AI has demonstrated its ability to detect abnormalities with unmatched accuracy and efficiency by utilizing sophisticated algorithms and machine-learning approaches.

The ability of artificial intelligence to identify complex patterns that may defy conventional fraud detection techniques is one of its primary advantages. Within big datasets, machine learning algorithms, especially those that employ unsupervised learning approaches, can detect minute deviations from typical behaviour [8]. These anomalies could include anomalous user behaviours, strange spending locations, or irregular transaction patterns. Artificial Intelligence is incredibly useful in detecting fraud that changes over time because of its capacity to automatically learn and adapt to new trends. Furthermore, AI systems are capable of taking into account numerous variables at once, such as user behaviour, transaction history, and contextual data. AI is able to examine intricate linkages and identify anomalies that might be signs of fraud, due to this approach. The continuous learning feature guarantees a dynamic defense against ever-evolving fraud schemes by ensuring that the system adapts to new threats. Several case studies show how AI can be used to spot irregularities and stop fraud in financial services.

The superiority of AI becomes clear when conventional approaches to fraud detection are contrasted with AI-driven alternatives. Existing techniques, which are frequently rule-based and dependent on predetermined standards, might encounter difficulty in adjusting to new fraud strategies [9]. Therefore, rule-based systems are less successful at recognizing complex constantly changing patterns since they usually set static thresholds for specific parameters. Conversely, AI uses dynamic algorithms that change in response to real-time inputs. Because of their flexibility, AI systems can respond to changing patterns and keep ahead of new fraud trends without the need for human intervention [10]. As such, AI-driven techniques are better at spotting irregularities and stopping fraud since they can analyze several variables at once, gain insight from past data, and recognize complicated linkages. Ultimately, the ability of AI to revolutionize fraud detection is demonstrated by the extent to which it can recognize abnormalities. AI strengthens the capacity to stop more complex fraud schemes by utilizing cutting-edge algorithms and machine-learning approaches.

## III. PREVIOUS WORKS ON FINANCIAL FRAUD DETECTION

Varmedja et al., [11] highlighted several techniques for classifying transactions as authentic or fraudulent. The credit card fraud identification dataset was used in the study. The dataset was quite imbalanced, so the SMOTE method was used to oversample it. Furthermore, the dataset was segmented into training and test data sets and attributes were selected. The technologies used in the study included Multilayer Perceptron, Random Forest, Naive Bayes, and Logistic Regression. According to the report, all technologies have a high degree of accuracy when it comes to identifying credit card fraud. Further abnormalities may be identified using the provided framework. Systems for identifying credit card fraud that uses supervised learning techniques operate under the premise that patterns of fraud can be discovered by analyzing previous transactions.

However, the process becomes more challenging when it has to take into consideration changes in customer behaviour and the ability of criminals to create new fraud patterns. In this case, fraud identification models can benefit from the use of unsupervised learning techniques to help them identify anomalies. A hybrid strategy for increasing the accuracy of fraud identification was presented by [12], with this approach incorporating supervised and unsupervised methodologies. Unsupervised anomaly ratings generated at different granularities on an actual, labelled credit card fraud identification dataset were analyzed and assessed. The experimental findings revealed that this combination is effective and increases identification accuracy.

According to [13], credit card fraud is detected using machine learning techniques. Initially, traditional approaches are applied. Following that, hybrid strategies that combine popular voting and AdaBoost are applied. The effectiveness of the framework is tested using a publicly available credit card dataset, and the data are then assessed using a real-time credit card dataset from a financial institution. Additionally, in order to assess the durability of the procedures, distortion is introduced into the data samples. The results therefore demonstrated that the popular vote method has a high degree of accuracy in identifying instances of credit card theft.

Many commercial banks have recently implemented a system to identify fraudulent activity by examining the cardholder's behaviour pattern. n the fraud detection process. Any transactions that deviate from the set pattern are identified and flagged by this analysis, making it possible to identify potentially dishonest activity [14]. This examination finds and highlights any transactions that fail to comply with the standard procedure. The application of the Hidden Markov Model, often known as HMM, is primarily linked to the e-sequence pattern of credit card transactions because HMM helps determine whether credit card fraud has been successfully committed, as evidenced by the findings of prior

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP1089

studies [15]. The earliest training of the Hidden Markov Model (HMM) is based on a typical transaction pattern associated with the specific cardholder. This analysis identifies and flags any transactions that deviate from the established pattern.

Economic fraud has proven to be dangerous and has affected the financial system significantly. One promising method in detecting credit card fraud in online transactions is data mining. Two problems have made credit card fraud identification challenging: the features of regular and fraudulent behaviour change over time, and the datasets used are heavily biased. The framework proposed by [16] aimed to compare the efficacy of different methodologies on credit card fraudulence data, including Logistic Regression, Naive Bayes, Random Forest, KNN, Multilayer Perceptron, Pipelining, and Ensemble Learning. Bagga therefore concluded that the variables used and the method used to identify fraud usually affect the efficacy of fraud identification.

## IV. AI ALGORITHM APPLICATION IN HEALTHCARE FINANCIAL FRAUD DETECTION

Several of the relevant literature offers a wealth of information on modelling techniques. Ko et al., [17] use a linear regression model and CMS Medicare Part B data from 2012 to simulate Medicare payments for Urologists as a function of the total number of patient visits. To find areas of overutilization and possible savings, actual payments are compared to estimated payments. Using the Part B data set, a prior study by [18] assessed deep neural networks and other methods for resolving class imbalance. Comprehensive coverage is given to data-level strategies for correcting class imbalance in the preprocessing phase.

When comparing supervised and unsupervised techniques for identifying fraud using CMS Part B data from 2015, [19] discovered that supervised learners outperform unsupervised learners by a large margin. The authors use manual feature selection to choose a collection of attributes that best describe provider claims after filtering the data to remove claims for prescription drugs. Branting et al., [20] use fraud labels from the LEIE and 2012–2014 Part B and 2013 Part D claims data from the CMS to extract characteristics from graph topologies. To classify fraud, behavioural similarity and geospatial co-location features are taken out of the network and modelled using decision tree learners.

Three methods were investigated by [21] for identifying fraudulent providers in Medicaid and Medicare claims data: temporal analysis for fraudulent provider identification, modelling provider interactions with graph networks, and modelling hidden themes using provider-diagnosis matrices. Although these linked efforts touch on various specific preprocessing processes and improve the state of machine learning-based healthcare fraud detection, they however lack sufficient information to be reliably reproduced.

For their Medicare fraud classification study, which applies a subset of the 2014 CMS Part B data, [22] provided relatively thorough preprocessing steps. They employed feature engineering to generate two new predictors: provider aggressiveness and the mean provider aggressiveness for each provider type procedure pair. Provider aggressiveness is an interaction term, which is defined as the ratio of the average submitted charge to the average payment amount. They impute missing values using the multivariate imputation by chained equations technique [23], and using the synthetic minority over-sampling technique (SMOTE) [24] to address class imbalance. The authors further augment the Part B data set with location features that capture patterns related to geographical variances in payments.

Van Capelleveen et al., [25] study fraud detection through a range of outlier detection algorithms using about a year of Medicaid dental data. The data set is cleansed of records with null values, zero-dollar payments, and future service dates. Preprocessing measures not listed here include deleting duplicate records and verifying the number of rows and schemas against supporting metadata. Healthcare financial fraud detection has greatly benefited from the use of AI algorithms, which offer more precise, effective, and scalable ways to spot fraudulent activity. Healthcare companies can address fraud from a variety of perspectives attributable to the distinct strengths and capabilities offered by machine learning, deep learning, and natural language processing algorithms. Even if there are still difficulties, mainly concerning bias, processing power, and data quality, the further advancement and application of these AI algorithms have enormous potential to improve fraud detection in the healthcare industry.

- *Future Directions*

The vast and intricate healthcare system in the United States is nevertheless susceptible to identity theft, billing fraud, and kickbacks, among other forms of financial fraud. In addition to costing billions of dollars annually, financial fraud erodes public confidence in medical organizations and the integrity of healthcare delivery [26]. The development of detection and prevention measures is required due to the growing complexity of fraudulent schemes. Algorithms based on AI have been demonstrated to be effective instruments for identifying and stopping financial fraud in the healthcare industry [27]. However, AI systems must be up-to-date with the ongoing evolution of fraud strategies. Potential future directions and technological developments in AI algorithms to counter financial fraud in the healthcare sector include: merging advanced machine learning methods, using explainable AI to promote trust and transparency, harnessing multimodal data analysis and natural language processing and improving cooperation and information exchange.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP1089

## V. CONCLUSION

The application of AI algorithms to combat financial fraud in the United States healthcare industry marks a revolutionary development in the ways that healthcare institutions can identify, stop, and handle fraudulent activity. Existing detection techniques are insufficient to handle the scope and complexity of the issue as financial fraud schemes become more complicated. By utilizing advanced machine learning, deep learning, and natural language processing techniques to evaluate enormous volumes of information, identify patterns, and detect anomalies indicative of fraud, artificial intelligence (AI) algorithms provide a potential alternative.

The review highlights important conclusions from evidence-based about how well AI detects healthcare fraud. Compared to human and rule-based techniques, AI algorithms can increase the accuracy and speed of fraud detection. AI models provide a flexible and adaptable solution that can tackle financial fraud, by gaining knowledge and adjusting to novel fraud patterns. In addition, while improving the detection of fraudulent activity, AI-driven fraud detection systems can help lower false positives and negatives, preventing the wrong flagging of legal transactions. However, there are challenges in using AI to detect healthcare fraud. To ensure the appropriate and ethical use of AI technology, issues on data quality, privacy, algorithmic bias, and the requirement for interpretability of AI models remain crucial problems that need to be addressed.

## REFERENCES


[1]. Sumalatha, M. R., & Prabha, M. (2019). Mediclaim Fraud Detection and Management Using Predictive Analytics. *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*. https://doi.org/10.1109/iccike47802.2019.9004241

[2]. National Health Care Anti-Fraud Association (NHCAA). (2023). *The Challenge of Health Care Fraud – NHCAA*. National Health Care Anti-Fraud Association. https://www.nhcaa.org/tools-insights/about-health-care-fraud/the-challenge-of-health-care-fraud/

[3]. Yelne, S., Chaudhary, M., Dod, K., Sayyad, A., & Sharma, R. (2023). Harnessing the Power of AI: A Comprehensive Review of Its Impact and Challenges in Nursing Science and Healthcare. *Cureus*, *15*(11). https://doi.org/10.7759/cureus.49252

[4]. Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Rab, S. (2022). Significance of machine learning in healthcare: Features, pillars and applications. *International Journal of Intelligent Networks*, *3*, 58–73. https://doi.org/10.1016/j.ijin.2022.05.002

[5]. Bekbolatova, M., Mayer, J., Ong, C. W., & Toma, M. (2024). Transformative Potential of AI in Healthcare: Definitions, Applications, and Navigating the Ethical Landscape and Public Perspectives. *Healthcare*, *12*(2), 125–125. https://doi.org/10.3390/healthcare12020125

[6]. Alowais, S. A., Alghamdi, S. S., Alsuhebany, N., Alqahtani, T., Alshaya, A., Almohareb, S. N., Aldairem, A., Alrashed, M., Saleh, K. B., Badreldin, H. A., Yami, A., Harbi, S. A., & Albekairy, A. M. (2023). Revolutionizing healthcare: the role of artificial intelligence in clinical practice. *BMC Medical Education*, *23*(1). https://doi.org/10.1186/s12909-023-04698-z

[7]. Ha, N., Xu, K., Ren, G., Mitchell, A., & Ou, J. Z. (2020). Machine Learning-Enabled Smart Sensor Systems. *Advanced Intelligent Systems*, *2*(9), 2000063. https://doi.org/10.1002/aisy.202000063

[8]. Bouchama, F., & Kamal, M. (2021). Enhancing Cyber Threat Detection through Machine Learning-Based Behavioral Modeling of Network Traffic Patterns. *International Journal of Business Intelligence and Big Data Analytics*, *4*(9), 1–9.

[9]. Kamuangu, P. (2024). A Review on Financial Fraud Detection using AI and Machine Learning. *Journal of Economics, Finance and Accounting Studies*, *6*(1), 67–77. https://doi.org/10.32996/jefas.2024.6.1.7

[10]. Abrahams, T. O., Ewuga, S. K., Kaggwa `, S., Uwaoma `, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Mastering Compliance: A Comprehensive Review of Regulatory Frameworks in Accounting and Cybersecurity. *Computer Science & IT Research Journal*, *5*(1), 120–140. https://doi.org/10.51594/csitrj.v5i1.709

[11]. Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M., & Anderla, A. (2019). Credit Card Fraud Detection - Machine Learning methods. *2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH)*. https://doi.org/10.1109/infoteh.2019.8717766

[12]. Carcillo, F., Le Borgne, Y.-A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2019). Combining unsupervised and supervised learning in credit card fraud detection. *Information Sciences*, *557*. https://doi.org/10.1016/j.ins.2019.05.042

[13]. Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2018). Credit Card Fraud Detection Using AdaBoost and Majority Voting. *IEEE Access*, *6*, 14277–14284. https://doi.org/10.1109/access.2018.2806420

[14]. Mohamadou, Y., Halidou, A., & Kapen, P. T. (2020). A review of mathematical modeling, artificial intelligence and datasets used in the study, prediction and management of COVID-19. *Applied Intelligence*, *50*. https://doi.org/10.1007/s10489-020-01770-9

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24SEP1089

[15]. Bhusari, V., & Patil, S. (2011). Application of Hidden Markov Model in Credit Card Fraud Detection. *International Journal of Distributed and Parallel Systems*, *2*(6), 203–211. https://doi.org/10.5121/ijdps.2011.2618

[16]. Bagga, S., Goyal, A., Gupta, N., & Goyal, A. (2020). Credit Card Fraud Detection using Pipeling and Ensemble Learning. *Procedia Computer Science*, *173*, 104–112. https://doi.org/10.1016/j.procs.2020.06.014

[17]. Ko, J. S., Chalfin, H., Trock, B. J., Feng, Z., Humphreys, E., Park, S.-W., Carter, H. B., Frick, K. D., & Han, M. (2015). Variability in Medicare Utilization and Payment Among Urologists. *Urology*, *85*(5), 1045–1051. https://doi.org/10.1016/j.urology.2014.11.054

[18]. Johnson, J. M., & Khoshgoftaar, T. M. (2019). Medicare fraud detection using neural networks. *Journal of Big Data*, *6*(1). https://doi.org/10.1186/s40537-019-0225-0

[19]. Bauder, R. A., & Khoshgoftaar, T. M. (2017). Medicare Fraud Detection Using Machine Learning Methods. *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*. https://doi.org/10.1109/icmla.2017.00-48

[20]. Branting, L. K., Reeder, F., Gold, J., & Champney, T. (2016, August 1). *Graph analytics for healthcare fraud risk estimation*. IEEE Xplore. https://doi.org/10.1109/ASONAM.2016.7752336

[21]. Chandola V, Sukumar, S. R., & Schryver, J. C. (2013). Knowledge discovery from massive healthcare claims data. *Knowledge Discovery and Data Mining*. https://doi.org/10.1145/2487575.2488205

[22]. Ekin, T., Frigau, L., & Conversano, C. (2021). Health care fraud classifiers in practice. *Applied Stochastic Models in Business and Industry*, *37*(6), 1182–1199. https://doi.org/10.1002/asmb.2633

[23]. Azur, M. J., Stuart, E. A., Frangakis, C., & Leaf, P. J. (2011). Multiple imputation by chained equations: what is it and how does it work? *International Journal of Methods in Psychiatric Research*, *20*(1), 40–49. https://doi.org/10.1002/mpr.329

[24]. Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic Minority Over-sampling Technique. *Journal of Artificial Intelligence Research*, *16*(16), 321–357. https://doi.org/10.1613/jair.953

[25]. Van Capelleveen, G., Poel, M., Mueller, R. M., Thornton, D., & van Hillegersberg, J. (2016). Outlier detection in healthcare fraud: A case study in the Medicaid dental domain. *International Journal of Accounting Information Systems*, *21*, 18–31. https://doi.org/10.1016/j.accinf.2016.04.001

[26]. Stowell, N., Pacini, C., Wadlinger, N., Crain, J., & Schmidt, M. (2020). Regulations Regulations Repository Citation Repository Citation. *William & Mary Business Law Review*, *11*(2), 11–2019. https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1189&context=wmblr

[27]. Johnson, J. M., & Khoshgoftaar, T. M. (2023). Data-Centric AI for Healthcare Fraud Detection. *SN Comput Sci.*, *4*(4). https://doi.org/10.1007/s42979-023-01809-x