SIN-CHN
SCIENTIFIC PRESS PTE.LTD.

AI Insights 2025, 1(1), 2001.
https://doi.org/10.62617/aii2001

Review

Machine learning techniques in healthcare provider fraud detection and analysis: A systematic literature review

Santhosh Chellappan[1,*], Ahmed AbuHalimeh[2]

[1] Department of Information Science, The University of Arkansas at Little Rock, AR 72204, USA
[2] Department of Computer & Information Science, The University of Arkansas at Little Rock, AR 72204, USA
*** Corresponding author:** Santhosh Chellappan, smchellappan@ualr.edu

CITATION

Chellappan S, AbuHalimeh A. Machine learning techniques in healthcare provider fraud detection and analysis: A systematic literature review. AI Insights. 2025; 1(1): 2001. https://doi.org/10.62617/aii2001

ARTICLE INFO

Received: 8 February 2025
Accepted: 20 March 2025
Available online: 11 April 2025

Abstract: Healthcare fraud is a growing concern, resulting in substantial financial losses and threatening the quality and trustworthiness of healthcare delivery. According to the National Health Care Anti-Fraud Association (NHCAA), healthcare fraud costs the economy tens of billions of dollars annually. Fraudulent activities, including upcoding, billing for unprovided services, and illegal kickbacks, contribute to rising healthcare costs, increased insurance premiums, and reduced quality of patient care. Combating healthcare fraud requires advanced detection systems, strict regulatory enforcement, and greater awareness among providers and patients. Machine learning (ML), a field within artificial intelligence, has emerged as a critical tool in healthcare fraud detection. This literature review examines the most recent scholarly articles on ML applications in fraud analytics, with a focus on (1) identifying and categorizing ML models used for provider fraud detection, (2) evaluating the effectiveness and challenges of ML-based approaches, and (3) exploring emerging trends and future advancements in fraud analytics. The findings reveal that supervised learning models such as Logistic Regression, decision trees, deep neural networks, and unsupervised techniques like anomaly detection and clustering are widely used to identify fraudulent patterns. Hybrid approaches that combine multiple ML models have demonstrated improved detection accuracy. Blockchain technology is an advanced database mechanism that, along with ML, can be used to improve the security, efficiency, and interoperability of healthcare data management and fraud detection. Nonetheless, there are still issues, including problems with data quality and standardization, data imbalance, evolving fraud tactics, and privacy concerns. This review study aims to assist researchers, professionals, and policymakers in implementing and managing machine learning models for fraud detection by providing insights into the key factors influencing these models. Understanding these factors will enhance decision-making in research projects and organizational operations, ultimately contributing to more effective fraud mitigation solutions in healthcare using state-of-the-art machine learning techniques.

Keywords: healthcare fraud detection; machine learning; blockchain; hybrid approaches; data complexity in healthcare; gaps; challenges

1. Introduction

Healthcare claims fraud causes significant financial losses for both the government and private citizens. Because of the volume of data produced by electronic health systems and the Internet of Things, as well as the rising complexity involved, fraud detection is becoming a more difficult task. Identifying fraud in healthcare programs is crucial, as an estimated 3%–10% of the total healthcare expenditures are lost to fraudulent activities [1]. The machine learning methods used to detect provider fraud in the health insurance industry are systematically reviewed in this article. We

aim to analyze the data and methodologies documented in the literature in recent years, providing insights into research challenges and opportunities.

The US Justice Department recently announced that as part of the 2024 National Health Care Fraud Enforcement Action, 193 defendants—including 76 doctors, nurse practitioners, and other licensed medical professionals—were charged with offenses in 32 federal districts around the United States. The defendants were accused of participating in several healthcare fraud schemes that resulted in around $1.6 billion in actual losses and $2.75 billion in intended losses [2].

Fraud prevention is an essential component of the maintenance of the structures of healthcare insurance. Therefore, health insurance fraud is a willful act in which the policyholder, healthcare practitioner, or insurance company intentionally provides false information in an attempt to get unjustified benefits or financial gains.

2. Background

The 2023 Health Care Fraud and Abuse Control (HCFAC) Program Annual Report, jointly released by the US Department of Justice (DOJ) and the Department of Health and Human Services (HHS), outlines significant advancements made in the fight against fraud, waste, and abuse across all federal healthcare programs. Overall, more than $3.4 billion was recovered, nearly twice as much as the year before. This surge can be attributed to several factors, including the restoration to full enforcement activity following pandemic-related slowdowns, a record number of high-value settlements under the False Claims Act, and the aggressive use of data analytics and Strike Force operations to target complex fraud schemes. The HHS Office of Inspector General (HHS-OIG) barred 2112 individuals and corporations from federal healthcare programs in FY 2023. Of these, 871 were exclusions based on criminal convictions related to healthcare programs, and 203 were the result of beneficiary abuse or neglect, both of which were mandated by law [3].

The charts below, **Figures 1** and **2**, show the number of individuals sentenced in connection with healthcare fraud and the median loss [4].

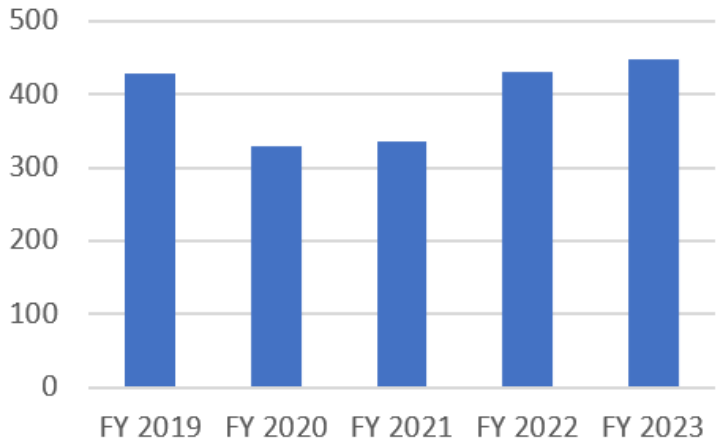

Figure 1. Number of individuals sentenced for healthcare fraud.

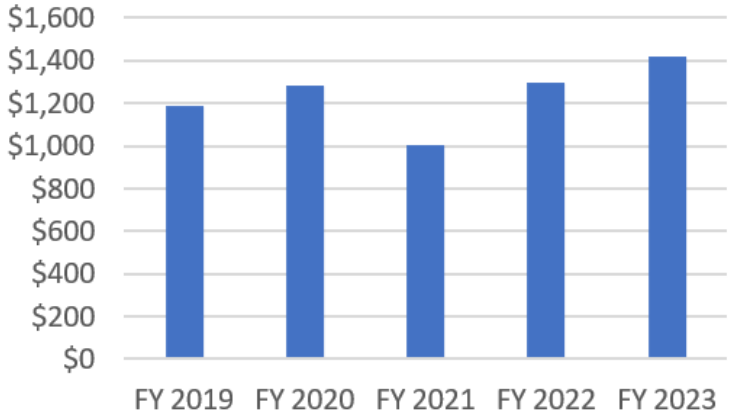

Figure 2. Median loss ($) for individuals sentenced for health care fraud.

As the bar chart in **Figure 3** shows, providers of Personal Care Services (PCS) participate significantly in fraud activities alongside other providers [5]. The pie chart below, **Figure 4**, also displays improper payments made by Medicaid, Medicare, and other programs [6].

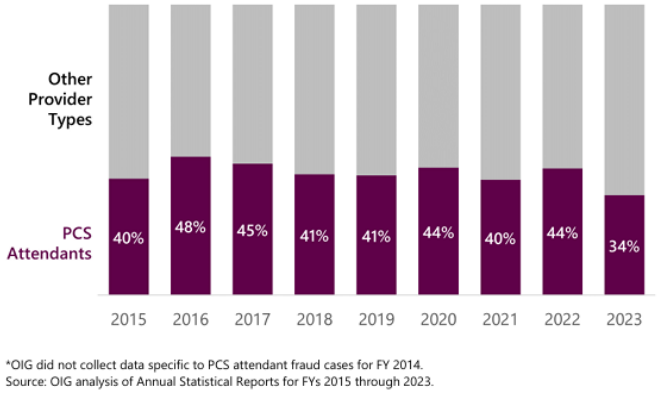

Figure 3. Fraud convictions among provider types during FYs 2015–2023.

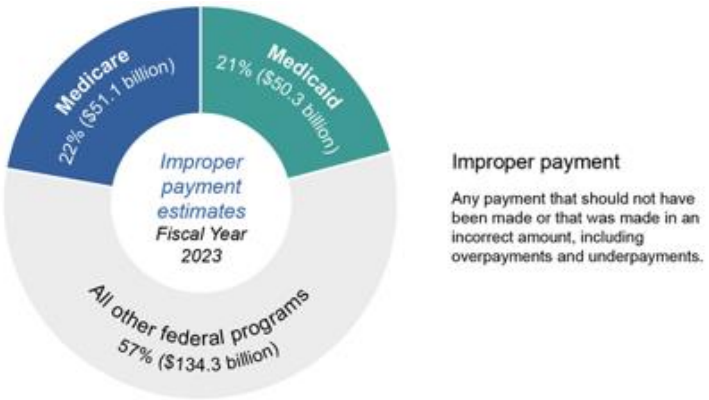

Figure 4. Improper payments estimate for fiscal year 2023.

The ability of computing systems to carry out operations commonly associated with human intellect, including learning, reasoning, problem-solving, perception, and decision-making, is known as artificial intelligence. Technological developments in artificial intelligence aid in the analysis of the vast amount of healthcare data in order to make well-informed decisions.

The purpose of this study is to discuss how artificial intelligence and machine learning can be used to identify and stop healthcare provider fraud. Deep Learning, supervised learning, and unsupervised learning can all be used to identify trends that might be linked to fraudulent conduct. These techniques make it possible to analyze vast volumes of data, learn from prior errors, and find intricate and nuanced patterns that are challenging to identify using traditional techniques.

Health insurance provider fraud frequently takes the form of billing for services or supplies that the patient never received, upcoding (billing for more costly services), unbundling (billing each procedure separately), double billing (submitting multiple/duplicate claims for the same service), kickbacks (payments for patient referrals), and falsifying medical records, among other practices.

This study will provide a detailed examination of various machine learning methods for provider fraud detection in the healthcare sector. In addition to Deep Learning techniques like neural networks, network graph analysis, and a combination of blockchain technologies, we currently conduct an experimental analysis of the most popular and effective ones, including clusters, Support Vector Machines (SVM), decision trees, Random Forests, and other conventional machine learning techniques. The results demonstrate how these cutting-edge machine learning algorithms can significantly reduce false positives and improve the early identification of fraudsters in claims processing, hence increasing the effectiveness of fraud detection systems. The ethical concerns, opportunities, and challenges of applying machine learning are also covered.

3. Literature review

This thorough analysis of literature examines 55 of the most recent scholarly articles out of the initial 100 articles on machine learning-based methods for detecting health insurance fraud from a variety of online sources, including IEEE Xplore, Elsevier, ResearchGate, Google Scholar, Springer, Springer Nature, Academia, and others. The review tries to find the gaps in the current approaches and how to close the gaps and improve the fraud detection process. Finding potential challenges in these areas and future paths in this crucial field are other goals of this review.

To understand insurance fraud and its effects on the global insurance market, Al Hosani et al. [7] conducted a bibliometric study. There were over 510 publications, and the study suggests that technological innovation can help lower insurance fraud, restore public trust, and involve companies in long-term social and economic projects that benefit society. Bibliometric studies often evaluate the consequences of citation and/or co-citation to have a better understanding of the issue. More than 100 studies on health insurance fraud detection using machine learning techniques from numerous globally renowned journals (the majority of which are from the United States) were systematically reviewed [8]. The findings indicate that the number of papers on machine learning for health insurance fraud detection has increased recently, particularly about identifying patient and healthcare provider fraud. This demonstrates how pertinent the subject of healthcare fraud and its repercussions is and that the primary perpetrators of the scam are healthcare providers.

Ali et al. [9] conducted a comprehensive assessment of articles concerning the use of artificial intelligence in the healthcare industry. The review initially looked at over 2000 papers from major scholarly databases before focusing on 180 articles for additional analysis to establish a classification framework that tackles the benefits, challenges, strategies, and features of AI-enabled health care. The review's findings demonstrate that AI is still far superior to humans in terms of precision, effectiveness, and timeliness when it comes to managing and analyzing medical and healthcare data.

A scoping review was performed by Iqbal et al. [10] to investigate the use of artificial intelligence in treatment settings for fraud detection. To locate pertinent scholarly articles, they used online search engines like Google Scholar and PubMed. Thirty-one of the 183 studies that were retrieved satisfied all requirements for inclusion. According to this study, AI has been used to identify various scams, such as identity theft and kickbacks in the medical field.

Fraud usually results from a combination of opportunity, pressure, rationalization, and capability [11]. Therefore, to effectively combat fraud, it is imperative to improve control and oversight, make investments in technology and education, and encourage cooperation with insurance organizations. The open research questions and concerns in the field of fraud detection with machine learning and Deep Learning algorithms are discussed [12]. These difficulties include the need for algorithms to be comprehensible and interpretable, the difficulty of managing datasets that are not balanced, the absence of shared datasets for comparing various methodologies, and the need for greater cooperation between academics and enterprises. By offering a structured framework for evaluating and comparing diverse approaches, researchers and practitioners are better able to comprehend the advantages and disadvantages of various strategies and contribute to the development of more potent fraud detection systems.

4. Research methodology

Beginning with the development of research topics, such as the types of health service fraud activities found in the corpus of recent literature, the study approach makes use of a comprehensive literature evaluation. Furthermore, the literature search was carried out using search terms such as "healthcare provider fraud," "health insurance fraud," or "machine learning applications for detecting healthcare fraud" across several online platforms, including IEEE Xplore, Elsevier, ResearchGate, Google Scholar, Elsevier, Springer, Springer Nature, Academia, and others. The following criteria were used to filter the chosen literature: 1) studies released in the last five years; 2) studies that mainly use data from US insurance systems, with other pertinent studies added based on their research methods and instruments because the US healthcare insurance landscape is very different from that of many other countries; 3) removal of duplicate entries; and 4) free full-text availability. The next step is to extract data from the selected publications, with an emphasis on the many kinds of provider fraud, the machine learning methods used in the studies, and the accuracy and precision of fraud detection attained by each of these models or methodologies.

For additional study, we have selected 55 articles from the original list of 100 publications that look at various machine learning models used to detect fraudulent activities.

The list of academic papers used for the literature review is displayed in **Table 1** below. The table lists the machine learning techniques applied in different studies along with the published sources. They are divided into various groups according to the study methodology. Definitions of various acronyms and keywords used in this review are shown in the Appendix (**Tables A1** and **A2**), listed at the end.

Table 1. Reviewed articles and methods.

Article	Methods	Model/Articles Group	Online source/Database
[7]	Bibliometric Correlations-Literature Review	Review Article	SSRN
[8]	Literature Review	Review Article	Elsevier
[9]	Literature Review	Review Article	Elsevier
[10]	Scoping Review	Review Article	Academia
[11]	Literature Review	Review Article	Semantic Scholar
[12]	Supervised Learning & Unsupervised Learning	Review Article	Springer Nature
[13]	NLP, Machine Learning & Artificial Intelligence	Conventional Machine Learning	ResearchGate
[14]	Machine learning, artificial intelligence, neural network	Conventional Machine Learning	Atlantis Press (Springer Nature)
[15]	Logistic Regression, Random Forest, Artificial Neural Networks (ANN)	Conventional Machine Learning	MDPI
[16]	Supervised, Unsupervised, and Deep Learning	Conventional Machine Learning	Elsevier
[17]	Decision Trees, Logistic Regression, Support Vector Machines (SVMs), K-Means Clustering, and Autoencoders	Conventional Machine Learning	Google Scholar
[18]	Regression analysis	Conventional Machine Learning	Google Scholar
[19]	Unsupervised machine learning, Isolation Forest, Apriori algorithm	Conventional Machine Learning	Springer
[20]	Sequential Forward Selection (SFS) method and SMOTE oversampling	Conventional Machine Learning	Semantic Scholar
[21]	Supervised learning, unsupervised learning	Conventional Machine Learning	Elsevier
[22]	AI and machine learning techniques	Conventional Machine Learning	Academia
[23]	Logistic Regression, Random Forest, Gradient Boosting, and Deep Learning (Convolutional Neural Network and Recurring Neural Network)	Deep Learning	Scientific Research Publishing Inc.
[24]	Machine Learning, Deep Learning	Deep Learning	Academia
[25]	Artificial Neural Network, Convolutional Neural Network	Deep Learning	Research Square
[26]	Nearest neighbor, SVM, Isolation Forest, one- class, SHAP	Deep Learning	ResearchGate
[27]	Neural Networks	Deep Learning	IEEE Xplore
[28]	Logistic Regression, Random Forest, Gradient Boosting, Embedding, Deep Learning	Deep Learning	IEEE Xplore
[29]	Artificial Neural Networks, Convolutional Neural Networks, Deep Learning with reinforcement learning.	Deep Learning	Google Scholar
[30]	Feature Engineering and Selection, ML, Decision Tree, Random Forest, XGBoost, SVM, Ensemble Models	Ensemble Modelling	Springer Nature
[31]	Feature Engineering, Random Forest, XGBoost, K-Fold- Cross-validation	Ensemble Modelling	Springer Nature

Table 1. (*Continued*).

Article	Methods	Model/Articles Group	Online source/Database
[32]	Synthetic Minority Over-sampling Technique (SMOTE), GNN, ANN, Random Forest, Logistic Regression, SVM, XGB	Ensemble Modelling	IEEE Xplore
[33]	Decision Tree, Random Forest, Graph Neural Networks, Reinforcement Learning, Federated Learning, XGBoost	Ensemble Modelling	ResearchGate
[34]	Ensemble Supervised Feature Selection (XGBoost, LightGBM, Extremely Randomized Trees, Random Forest, and CatBoost, Explainable Machine Learning	Ensemble Modelling	Springer Open
[35]	Random Forest, Logistic Regression, SVM, Deep Learning, Ensemble Approach	Ensemble Modelling	IEEE Xplore
[36]	Multiple unsupervised machine learning algorithms (Isolation Forest, KNN, SVM, Majority Voting technique)	Ensemble Modelling	Elsevier
[37]	Ensemble machine learning models	Ensemble Modelling	Springer
[38]	Feature Selection, Embedded methods	Ensemble Modelling	Research Square
[39]	Gradient Boost Tree, XGBoost, CatBoost, and Random Forest models, Bagging algorithms	Ensemble Modelling	IEEE Xplore
[40]	Random Undersampling, Ensemble Supervised Feature Selection	Ensemble Modelling	Springer Nature
[41]	K-nearest neighbor (KNN), Logistic Regression (LR), Support Vector Machines (SVM), Extreme Gradient Boosting (XGB), Multilayer Perceptron (MLP), Ensemble modeling	Ensemble Modelling	Google Scholar
[42]	Ensemble Machine Learning	Ensemble Modelling	PubMed
[43]	Bayesian Belief Network (BBN)-Graphical Network Model	Graph/Network Model	Elsevier
[44]	Graph Attention Networks, (Feed Forward Neural Network)	Graph/Network Model	IEEE Xplore
[45]	Graph Neural Networks	Graph/Network Model	IEEE Xplore
[46]	Isolation Forest, Graph-Based Social Network Analysis (SNA)	Graph/Network Model	IEEE Xplore
[47]	Network analytics, Graph Neural Networks (GNN), GBA	Graph/Network Model	Springer
[48]	Graph Analytics, Machine Learning	Graph/Network Model	Academia
[49]	Graph Analysis	Graph/Network Model	IEEE Xplore
[50]	Heterogeneous information network	Graph/Network Model	Springer
[51]	Machine Learning & Blockchain technologies, Hyperledger fabric	ML & Blockchain Technologies	Elsevier
[52]	Machine Learning, Ensemble Learning, Blockchain	ML & Blockchain Technologies	Elsevier
[53]	Machine Learning & Blockchain Framework	ML & Blockchain Technologies	IEEE Xplore
[54]	Blockchain Technology and Self-Sovereign Identity (SSI),	ML & Blockchain Technologies	Elsevier
[55]	Blockchain with Machine Learning	ML & Blockchain Technologies	ResearchGate
[56]	KNN, K Means, Decision Tree Classifier, Random Forest, XG Boost, Gradient Boosting, and Blockchain technologies	ML & Blockchain Technologies	IEEE Xplore
[57]	Blockchain technologies and AI	ML & Blockchain Technologies	ResearchGate
[58]	Binary Logistic Regression	Conventional Machine Learning	Scopus
[59]	XGBoost	Ensemble Modelling	Google Scholar
[60]	Decision Tree, Random Forest, Support Vector Machine	Conventional Machine Learning	Elsevier
[61]	Supervised Learning & Unsupervised Learning	Review Article	ResearchGate

Note: AI—Artificial intelligence, ML—Machine learning, ANN—Artificial Neural Network, CNN—Convolutional Neural Network, GNN—Graphical Neural Network, LR—Logistic Regression, RF—Random Forest, SVM—Support Vector Machine.

Figure 5 below shows the articles by machine learning methods or by the article group, and **Figure 6** shows the number of articles selected for the study from the last 5 years.

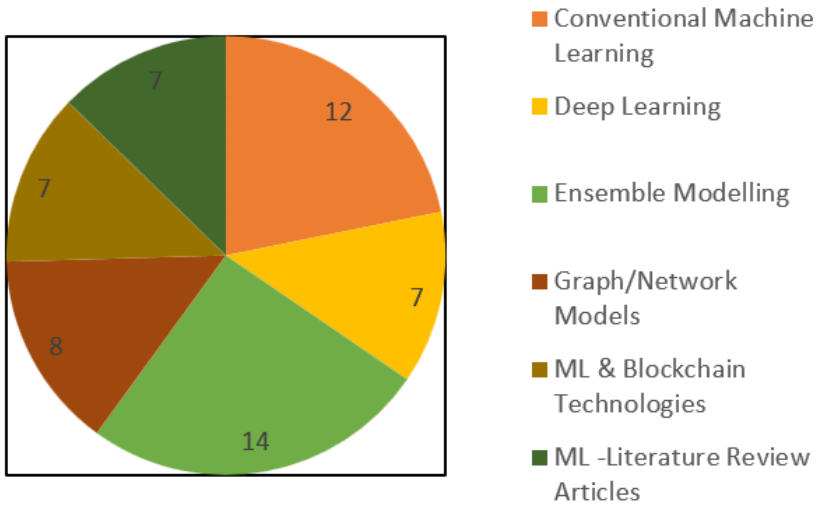

Figure 5. Number of publications by methods/types.

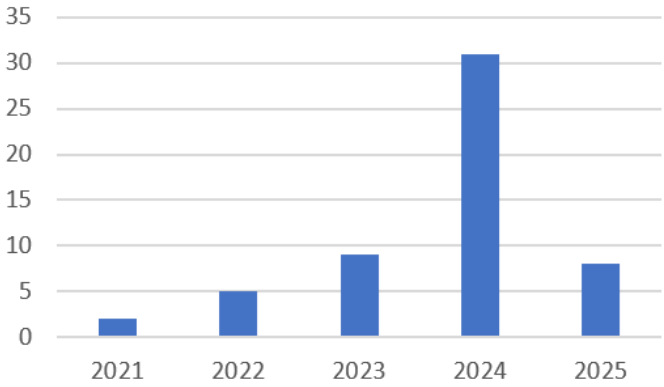

Figure 6. Number of publications.

Figure 7 depicts the research steps, which include searching various articles on machine learning methods for provider fraud analytics on online resources and identifying the most relevant articles on recent advances in machine learning applications. The study compares different models and groups based on the type of models used, identifying the challenges and future directions in this critical area.

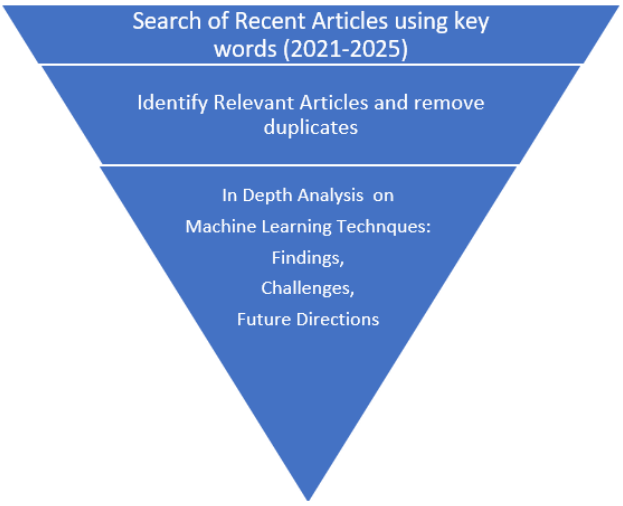

Figure 7. Research steps.

Based on the methods employed in the research, these publications are categorized into five groups. 1) Conventional approaches for machine learning, 2) Deep Learning methods, 3) Ensemble modeling, 4) Graph network analysis, 5) Blockchain technologies. Many of these articles combine different machine learning approaches in their research.

4.1. Conventional machine learning

Conventional machine learning techniques include classification, regression, and clustering. They also include data analysis methods such as Logistic Regression, decision trees, linear regression, and K-Nearest Neighbors.

Machine learning, Natural Language Processing (NLP), and artificial intelligence are examples of advanced data analytics technologies that can significantly increase the accuracy of provider healthcare fraud analytics [13]. Applications of artificial intelligence that identify fraudulent activity in insurance claims are examined in another study [14]. The machine learning models greatly increase prediction accuracy and overall efficiency. The benefits and drawbacks of the current machine learning-based fraud detection techniques are also covered in the article.

Models including Logistic Regression, Random Forest, and Artificial Neural Networks are examined in the study of Saudi Arabian provider fraud [15]. To deal with the imbalanced dataset, they employed the Synthetic Minority Oversampling Technique (SMOTE) approach. To exclude irrelevant characteristics, feature selection was used. Accuracy, precision, recall, specificity, F1 score, and Area Under the Curve (AUC) are then checked as part of the validation process. A study on the use of machine learning (ML) and artificial intelligence (AI) for improved fraud detection and prevention in Nigeria was carried out [16]. They have investigated a variety of Deep Learning approaches as well as supervised and unsupervised methods. The study demonstrates how these models can be applied to network analysis, risk assessment, behavioral analysis, and anomaly identification. The study emphasizes the advantages of machine learning in fraud detection, such as increased accuracy and efficiency.

According to Azad and William [17], anomaly detection can be utilized to spot fraudulent activities, including upcoding, phantom billing, kickbacks, etc. Predictive

analytics and Natural Language Processing (NLP) tools improve the accuracy of fraud detection. To promote a culture of alertness and compliance and, consequently, lower fraud activities, the study also highlights the significance of policy efforts, such as improved staff training and inter-organizational coordination.

The implementation of AI-based fraud reduction tactics may have a substantial impact on the healthcare industry, according to a quantitative analysis of research data [18]. Therefore, healthcare businesses may preserve patient data, uphold public trust, and preserve their financial resources by improving and automating fraud detection skills. Additionally, the proposed results show how AI can help raise awareness about healthcare fraud prevention, resulting in a safer and more efficient healthcare system. To detect healthcare insurance fraud, the study [19] presents a fraud detection system that makes use of unsupervised learning and association rule mining approaches.

The suggested methodology operates in two stages, and the Center of Medicare & Medicaid Services (CMS) dataset is used for analysis. First, frequent rules based on patient, service, and service provider characteristics are extracted from the transactions using association rule mining. Second, to detect fraudulent activity, these rules are fed into unsupervised classifiers.

Another study used 27 pertinent studies out of 450 publications to evaluate methods and findings from various academic fields [20]. The primary focus was healthcare fraud, with an emphasis on addressing the gaps and constraints present in the corpus of current literature. The study offers a Sequential Forward Selection (SFS) method with SMOTE oversampling for classification using a bagging classifier and a stacking meta-estimator, and fraud detection using K-Nearest Neighbors, Artificial Neural Networks, Linear Discriminant Analysis, and Gradient Boosting Machines.

An unsupervised multivariate analysis model uses Weighted MultiTree (WMT) for categorical data to examine provider and service provider similarity to identify fraudulent services. By applying multiple Density-Based Clustering (DBC) approaches to continuous data of claims, including service counts and service costs, it uses a univariate fraud detection model to identify false claims [21].

The article by Sharma et al. [22] investigates the possible uses of AI-powered fraud detection systems in SAP for research in retail and healthcare. According to the study, enhanced machine learning provides cost savings, real-time transaction and activity monitoring, and improved precision and accuracy. They examined several models, their difficulties, and fraud detection success rates.

4.2. Deep Learning

A subset of machine learning known as “Deep Learning” simulates the intricate decision-making process of the human brain by using multilayered neural networks, or “deep neural networks.”

Provider fraud can be effectively detected using Random Forest, Logistic Regression, and Deep Learning (Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) [23]. Simply put, the recommended approach produced fewer false positives. Receiver Operating Characteristic (ROC) analysis is used to establish the relationship between the true positive rate and the false positive rate. It has been demonstrated that ensemble techniques like Random Forest and

XGBoost exhibit exceptional precision and recall, rendering them appropriate for fraud scenario detection with few errors. CNNs and RNNs are two examples of Deep Learning methods that produce higher recall and precision scores. A study by Das and Krishna Bhat [24] looks at how AI-powered strategies could be used to stop fraud and provide best practices for employing models in their efforts to detect fraud. Machine learning significantly aids in early fraud discovery during the intake and claims processing stages of insurance operations.

Three Deep Learning models—long short-term memory networks (LSTM), Convolutional Neural Networks (CNN), and Artificial Neural Networks (ANN)—are examined in another study [25]. To investigate the use of healthcare services and spot fraudulent conduct, this study looked at information from healthcare claims, such as patient demographics, claim amounts, diagnostic codes, and procedure kinds. Additionally, locally interpretable model-agnostic explanations (LIME) were employed to make these models more comprehensible.

The workflow for explainable anomaly identification in the healthcare insurance industry is investigated by De Meulemeester et al. [26]. The approach makes use of cutting-edge machine learning techniques that are novel in healthcare insurance identification, such as SHapley Additive exPlanations (SHAP) explainability, categorical embeddings, and state-of-the-art anomaly detection techniques. Mayaki and Riveill [27] discussed about the high dimensionality and class imbalance of the Medicare Part D data. The team used feature selection, Random Under Sampling (RUS), and a combination of feature selection methods. Six machine learning classifiers were evaluated for Medicare fraud detection using the Area Under the Precision-Recall Curve (AUPRC) and Area Under the Receiver Operating Characteristic Curve (AUC).

Fursov et al. [28] suggested an option to use tabular data to build models that can distinguish between fraudulent and authentic claims. Deep Learning architectures that leverage consecutive patient visits and characteristic information have been discussed. It can provide fresh perspectives on identifying health insurance fraud, and the findings indicate that this method performs better than alternative models and can significantly enhance the claims-handling procedure. Studies showed that ANN is highly effective at analyzing structured numerical data and detecting fraudulent claims by looking at transaction patterns, provider behavior, and billing anomalies. They proposed merging rule-based systems, CNN, and ANN to increase the accuracy of fraud detection. Fraud activity can be dynamically detected by combining Deep Learning with reinforcement learning [29].

4.3. Ensemble modelling

A machine learning-driven automated approach is presented by Devaguptam et al. [30] with the goals of minimizing financial losses in the insurance industry, identifying high-risk clients, preventing fraudulent claims, and minimizing human participation. The framework first focuses on detecting fraud to determine the accuracy of claims. In actual claims, the patient's medical history determines premiums and related risk factors. Ensemble modeling is a machine learning technique that builds a better, more accurate model by combining the predictions of several

separate models. Several ensemble approaches and machine learning-based classification models were used and assessed.

Johnson and Khoshgoftaar [31] used CMS public claims data to explore a data-centric approach for their study. They produced six new Medicare data sets with labels, including the Aggregated Enriched and Summary by Provider data sets. Results like Area Under Curve (AUC), True Positive Rate (TPR), True Negative Rate (TNR), and Geometric Mean (G-mean), among others, demonstrate how much better the aggregated-enriched data set performs than the conventional techniques. To address the class imbalance, Chirchi and Kavya [32] explained how to use Random Forest, Logistic Regression, XGBoost, and SMOTE to identify behavior patterns of the providers. They evaluated each model's performance using confusion matrices, accuracy, sensitivity, specificity, Kappa values, AUC, and F1 scores. They claim that SMOTE improves model robustness, which in turn improves fraud detection capabilities and, as a result, lessens the effect of fraud on medical expenses.

A study by Narne [33] asserts that although machine learning methods can identify fraud, more sophisticated methods, such as Explainable AI (XAI), supervised and unsupervised learning, and ensemble methods, offer accuracy and transparency while building stakeholder trust.

Medicare fraud can be effectively detected using the ensemble-supervised feature selection method. By classifying highly unbalanced big data, a supervised machine learning technique known as anomaly detection can be used to detect Medicare insurance fraud. Feature selection is an essential step in improving the effectiveness of model training and developing more understandable machine learning models for fraud detection. Without compromising effectiveness, the feature selection approach reduces the dimensionality of the dataset [34].

The stacking ensemble model [35] proved to be especially effective, outperforming the others in terms of accuracy. Transparency is essential for the real-world implementation of these models in healthcare systems, and SHAP value analysis has added an interpretability layer.

The research [36] has created an ensemble of eighteen new unsupervised algorithms, specifically anomaly detection models, that are used in advanced fraud detection. The majority voting method used to combine the results from these many algorithms is innovative and improves the accuracy and dependability of fraud detection. Two methods are used to validate the suggested system. To establish a performance criterion for the model, human medical insurance experts first review a sample of claims. Second, the system's effectiveness is quantitatively assessed using significant statistical measures. The system makes use of actual insurance claim data from Gulf nations to ensure quality and applicability. An article by Talukder et al. [37] employs an integrated multistage ensemble machine learning (IMEML) model to enhance fraud identification. Several multistage ensemble models, such as Ensemble Independent Classifier (EIC), Ensemble Bagging Classifier (EBC), and Ensemble ML Classifier (EMC), are integrated into this model. In terms of performance parameters like accuracy, precision, recall, f1-score and AUC score, among others, the suggested model performs better than traditional machine learning models.

Another example [38] looked at machine learning techniques to enhance model performance and fraud detection precision in their research paper. They used feature

selection techniques, including embedding methods and permutation importance, in addition to model fusion techniques like weighted, stacking, and voting. To further increase the model's decision-making dependability and transparency, interpretability techniques such as Partial Dependence Plots, SHAP, and LIME were used. The outcome is an interpretable, high-performing model that greatly enhances health insurance fraud detection.

Yao et al. [39] developed a Medicare fraud detection model using the Bagging technique. Considering their proven efficacy in past research, the Gradient Boost Tree, XGBoost, CatBoost, and Random Forest models serve as the foundation for the Medicare fraud detection model. They introduced the Bagging algorithm, which is based on the weighted threshold technique called WTBagging, and used the Bagging and WTBagging methods to build ten model combinations.

Studies also attempted to classify extremely unbalanced big Medicare data using machine learning models to detect fraud [40]. showed that data reduction strategies greatly enhance classification performance using two CMS datasets and the List of Excluded Individuals/Entities (LEIE) for the study. To overcome the problems of class imbalance and the exclusive focus on blatantly fraudulent providers, Tajrobehkar et al. [41] used the expertise of seasoned doctors and medical billers to produce a labeled dataset. The study's objective was to assess various machine learning models to identify the most effective screening method for identifying Medicare overutilization in ophthalmology. The unique accomplishment of this objective was made possible by the development of a large labeled dataset of ophthalmologists. By addressing the issue of class imbalance and identifying subtle fraudulent patterns and overutilization, their medical team made sure that the labeled dataset addressed the limits of the LEIE dataset. By utilizing the advantages and varied viewpoints of numerous machine learning models, they discovered that the stacking ensemble model improved overutilization detection. Data preprocessing, model integration and training, and outcome analysis with feature interpretation comprise the methodology [42]. They compared the results of their many model combinations using ensemble techniques, such as voting, weighted, and stacking procedures. Partial Dependence Plots (PDP), SHAP, and LIME were used to interpret the attributes, enabling us to see how each characteristic affected the predictions.

4.4. Graph or network analysis

According to Kumaraswamy et al. [43], to improve fraud detection at an earlier stage, the relationships between the several parties involved in healthcare payment transactions must be taken into consideration. Analysis should be done on the patient, payer, or provider's combined engagement. They devised a graphical network model called the Bayesian Belief Network (BBN), which exploits the relationship structure of characteristics in a transaction and offers better interpretability qualities than many other machine learning techniques. It is difficult for end users to assess fraud detection techniques due to the interpretability of machine learning models. The suggested model was assessed using quantitative comparisons such as unequal class distribution, variable discretization, and the impact of parameter adjustment. This model is very simple for auditors and investigators to understand. Examining claims data alone will

not provide a complete picture of the fraud operations. The fraud activities may include many parties [44].

To identify the underlying reason for fraudulent activities, it is essential to examine the relationships between patients, doctors, and healthcare professionals, among others. They talked about a strategy for detecting healthcare provider fraud that uses a feed-forward neural network to classify data and a graph attention network to incorporate the interactions of various parties. To improve the fraud detection model's effectiveness, they have incorporated both relational and intrinsic features.

A study [45] claims that the performance of Medicare fraud detection models can be improved by using graph neural networks on graph structured datasets. The GraphSAGE algorithm and a graph neural network are used to graph-structured datasets created from open-source data, such as Medicare beneficiary, provider, and physician data, in this article's Medicare fraud detection model. Medicare beneficiaries and providers were designated as nodes, resulting in a heterogeneous graph. In terms of F1 score, precision, recall, and area under the receiver operating characteristics curve, the GraphSAGE model thus performed better than the baseline model.

Graph-Based Social Network Analysis (SNA) to detect health insurance fraud is discussed in this article [46]. Utilizing the interdependence of policyholders, medical professionals, and other pertinent parties, our method produces a comprehensive graph representation that captures the intricate network dynamics present in the health insurance system. Fraudulent activity is detected using an anomaly detection algorithm and careful node and edge attribute creation to spot subtle patterns. The results demonstrate the efficacy of the proposed methodology and its superiority over the alternatives. The study's contributions to methods for identifying health insurance fraud improve the system's integrity and cost-effectiveness. Given the ongoing seriousness of health insurance fraud, this study provides practitioners and industry authorities with a thorough and relevant response.

The use of network analytics for fraud detection was elaborated by Deprez et al. [47]. Complex patterns that are suggestive of fraud are identified through the interactions between several entities. To evaluate the predictive power of various approaches against one another, the literature first evaluated and applied them in the context of insurance fraud. To identify fraud, they prioritized network features above intrinsic ones. In contrast to other claim-specific models, their study found that while sophisticated methods may not always perform better than simple network features, they do aid in the detection of various fraud patterns. Machine learning and graph analytics are excellent options for precisely identifying false assertions [48]. utilizing this expanded information to guide machine learning and display the data as a graphical network. These techniques are more accurate than traditional methods and can optimize the fraud detection process in health insurance claims.

According to Yoo et al. [49], Medicare fraud detection can be improved by incorporating graph analysis that considers the relationships between physicians, beneficiaries, and medical providers. They created a graph structure by combining information about possible fraudulent providers, inpatient and outpatient claims, and beneficiary data. By employing graph centrality measures, the two models—a graph neural network (GNN) model and a classical machine learning model—display much

better performance outcomes than the GNN model. MHAMFD, a multilevel attention mechanism-based model, is explored [50] as a means of identifying health insurance fraud. This selects the appropriate neighbor nodes based on the behavioral relationships at different points during a patient's visit. They have developed a hierarchical attention method to gather complex semantic information from the interlacing of different patient behavioral encounters. This makes the model interpretable and enhances the feature representation of objects by identifying the main causes of fraud.

4.5. Blockchain technologies

Blockchain technology and machine learning methods (Random Forest Regression and Support Vector Machine (SVM)) can be used to detect fraudulent payments [51]. Blockchain technologies also help to protect private patient data and health insurance records. They suggested an integrated framework that outperforms conventional techniques and is more reliable and effective. By creating a distinct digital identity for each patient, blockchain technology can help decrease identifying errors. The report describes how the hospital and insurance consortium are connected using a private blockchain called Hyperledger fabric. Hyperledger fabric-permitted, immutable networks provide superior data integrity, scalability, and cost reductions. The study [52] describes a blockchain-enabled method for healthcare insurance claim fraud detection that is based on ensemble learning. Strong data security is ensured by utilizing blockchain technology, protecting patient data and private medical records. The evaluation demonstrates the methodology's effectiveness (using blockchain and ensemble learning techniques) in comparison to traditional machine learning algorithms. This system offers a more comprehensive approach to claim fraud detection by integrating beneficiary, in-patient, and out-patient data. Accuracy, precision, recall, Receiver Operating Characteristic (ROC), and other performance indicators were used to assess the model.

The article by Selvamuthu et al. [53] examined a new blockchain-based system that is combined with machine learning methods to identify and prevent healthcare fraud. K-Nearest Neighbors (KNN), Naive Bayes, Logistic Regression, Decision Tree, Support Vector Machine (SVM), AdaBoost, Gradient Boosting Machine (GBM), Convolutional Neural Network (CNN), and Recurrent Neural Network (RNN) are among the nine prior models that are compared to the suggested model. The findings demonstrate that the suggested model performs noticeably better than the top-performing models currently in use in machine learning. Blockchain technology reduces processing time and increases the security and transparency of the claims process. This study shows how blockchain technology, in conjunction with AI and machine learning, has the potential to revolutionize the health insurance industry by offering a dependable and efficient way to handle claims and stop fraud. SSI-MedRx, a healthcare system that makes use of Self-Sovereign Identity (SSI) and blockchain technology to protect patient privacy, secure interoperability, and stop difficult healthcare frauds like opioid overprescribing, phantom billing, medical identity theft, and kickbacks [54]. By giving individuals greater control over their health and

personal information, this design can lower the risk of data breaches and enhance care coordination.

Research published by Gupta et al. [55] combines machine learning methods for fraud detection with a blockchain-based system for handling health insurance claims. Another study [56] handled medical data in a private and secure environment to reduce the risk of fraud. The approach is based on leveraging the Ethereum blockchain to increase the power of complex machine learning models. They used Ganache, a private blockchain created by Ethereum and backed by the Pinata service, to securely store data from a blockchain perspective. They also look at personal insurance plans and use machine learning models to identify any fraud. The use of blockchain and machine learning to address privacy and fraud detection in health insurance is covered in the article by Mani et al. [57]. For strong fraud detection systems and cyberthreat defenses, they have suggested blockchain and artificial intelligence (AI)-driven design.

5. Results and findings

The primary foundation of healthcare fraud detection algorithms is the use of machine learning techniques for payer-claims data exchanges to identify fraudulent activity. The interconnections that naturally exist in the claims generated from a single unit, such as the patient, payer, or provider, are typically overlooked when analyzing claim transactions in isolation.

Many fraud detection methods solely analyze claims data. It is important to consider the relationship between healthcare providers, doctors, and patients because healthcare fraud can involve multiple parties. Investigating the critical function of machine learning models and their potential applications in tackling the fraud problem is the aim of this study. Intentionally filing false claims or fabricating information to receive entitlement payments is known as healthcare fraud. For this reason, it is crucial to improve oversight and control, make investments in technology and education, and encourage cooperation with insurance companies to effectively fight fraud. The Medicare system's healthcare provider fraud presents a significant obstacle to the healthcare industry, which is essential to society's well-being. It has been shown that the binary Logistic Regression fraud detection model may successfully identify fraudulent healthcare transactions that need exact identification [58]. One popular application of the gradient boosting technique, especially in machine learning contests, is called XGBoost (Extreme Gradient Boosting). It is well known for its excellent performance and effective deployment on distributed and multicore computers [59].

Studies have shown that Deep Learning and ensemble modeling increase the capacity to anticipate fraudulent activity. The graph network model further improves accuracy and precision. The hybrid approach, which combines blockchain technology with machine learning techniques, provides more security features and early fraud detection from claims.

Many fraudulent activities in healthcare claims and improper patient data processing have been reported in the healthcare insurance industry. Manual processes or procedures to analyze large amounts of healthcare data limit the ability to find fraudulent activities. Successful integration of technologies and the use of artificial

intelligence will help to improve healthcare claims management and detect unusual behaviors in claims transactions. However, this requires careful consideration of ethical issues, including data privacy and model transparency. Machine learning and artificial intelligence technologies will play a crucial role in detecting healthcare fraud activities and ensuring the integrity of healthcare insurance systems [60].

The healthcare insurance industry is continuously looking for solutions to detect fraudulent claims. Traditional techniques for identifying insurance fraud are not very effective in the current digital world. Methods for detecting insurance fraud are being revolutionized by recent advancements in artificial intelligence and machine learning. These papers cover a broad range of machine learning algorithms that employ supervised, unsupervised, and hybrid techniques.

6. Gaps, challenges, and opportunities

The study of provider fraud detection is significantly hampered by the complex structure of healthcare claims data. Multi-modality, heterogeneity, and non-stationarity are characteristics of this data, which frequently shows large dimensionality and size, lacks standardization, and is not integrated. These difficulties are made worse by the scarcity of ground truth labels for fraud, which continues to be a significant barrier to the deployment and validation of machine learning (ML) models for the identification of fraudulent activity.

To summarize the techniques and strategies employed, several articles on healthcare fraud detection were examined. They discovered that no one procedure unifies different research techniques to detect healthcare fraud. They also observed that the different data sources used for the study have a significant impact on feature engineering [61]. The actions required following fraud detection are not covered in most of the literature on fraud detection. Integration of data from multiple sources often raises concerns over the data quality [62]. The accuracy and completeness of data are crucial factors for any machine learning model.

Issues with fraud detection systems driven by AI: despite being powerful tools in the fight against fraud, machine learning (ML) and artificial intelligence (AI) face challenges in their implementation. Organizations must be prepared to handle a range of obstacles when using AI-powered fraud detection systems, from technological limitations to legal concerns.

Data regulations and privacy issues complicate the issue by potentially limiting the number of large datasets that AI systems can access to ensure data integrity and comply with privacy regulations. It will be difficult to integrate modern AI and ML technologies with existing infrastructure and historical systems, necessitating significant changes or even whole rebuilds. Because of the growing cybersecurity threats to healthcare, a stronger regulatory framework needs to be created in order to protect patient data, meet security standards, and lessen the exposure of institutions. To provide sufficient cyber protection, healthcare institutions need to comply with more than just HIPAA (Health Insurance Portability and Accountability Act, a US federal law for safeguarding patient privacy and ensuring the security of medical records), GDPR (General Data Protection Regulation, a European Union law that establishes rules for how businesses may gather and utilize personal data), and NIST

(National Institute of Standards and Technology) cybersecurity rules [63]. GDPR requires businesses to have strict data protection safeguards in place and highlights people's rights to control their personal data. In order to reconcile compliance with efficient fraud detection in this legal climate, sophisticated data anonymization and encryption solutions are required. The regulatory landscape in the United States is more disjointed, with state-specific regulations complementing federal statutes such as the Affordable Care Act (ACA) and HIPAA. For insurance firms that operate in several states, this results in a complicated compliance environment.

Similar to the EU, the U.S. framework places a strong emphasis on data security and privacy, but it also has special measures to fight healthcare fraud, such as the HCFAC (Health Care Fraud and Abuse Control Program) program [64]. Asia-Pacific nations, like Australia and Japan, have their own regulatory systems that strike a compromise between preventing fraud and protecting data. Establishing and implementing legislative frameworks for medical insurance fraud detection presents particular difficulties for developing nations.

Because the patterns of fraud operations are always changing, machine learning models need to be continuously trained. There are ethical concerns with using AI to make decisions. Businesses must carefully handle a variety of moral and legal situations when utilizing AI for fraud detection to maintain moral principles and guarantee compliance.

The study by Islam Prova [35] explains the need for real-time, instantaneous and reliable healthcare fraud detection capabilities within healthcare systems. The goal is to identify fraud as quickly and accurately as possible so that any losses can be and valid claims can be handled right away. Continuous monitoring and evaluation of the healthcare systems are needed to ensure their effectiveness and adapt to changing fraud patterns.

Computational resource constraints like memory, CPU, execution time and scalability should be considered while selecting different ML techniques. Training models for detecting fraudulent claims patterns requires substantial memory to store sequential data and computational power for backpropagation. Detecting collusion in fraud networks using GCNs can be computationally expensive due to the need to aggregate information from neighboring nodes. Reduce data dimensionality using PCA or feature selection, Model Pruning, parallel processing, CPU speed acceleration, Hyperparameter Optimization, etc. These are some of the techniques to optimize the computational resources. ML models need to be designed and deployed in a way that protects patient privacy while still allowing effective fraud detection.

By developing explainable AI models, users may better understand how decisions are made and increase accountability and transparency. Decision Trees, neural networks, and meta-learning can be used to explain reasons behind predictions. Models Feature selection techniques can be employed to generate more explainable models, as well as significantly decrease the size of a highly imbalanced big data dataset without necessarily compromising classification performance [34].

Explainable Artificial Intelligence (XAI) techniques can be used to provide insights into the reason why a model determines false claims. The claim investigators can use these explanations as a starting point, which cuts down on the amount of time they need to inspect. The SHapley Additive exPlanations (SHAP) from the meta-

learning model provide a straightforward explanation of the logic involved in the fraud detection [26,35,38,65]. SHAP assigns each feature an importance value for a particular prediction and helps investigators comprehend the rules and criteria behind a particular claim's flagging. By using an interpretable model to approximate the model locally, LIME (Local Interpretable Model-Agnostic Explanations) provides an explanation for each specific prediction. Along with improving detection capabilities, integrating these XAI approaches into fraud audits and claims processing systems guarantees that the decision-making process is clear and intelligible to all parties involved.

Table 2 below depicts the current gaps in healthcare data analysis, the challenges in using AI and ML techniques, the legal and regulatory restrictions, and the many security, privacy, and ethical issues. It also outlines the future steps to address these gaps and enhance healthcare data analysis.

Table 2. Healthcare fraud detection: Gaps, challenges, and future directions.

Category	Gaps & Challenges	Future Directions
Standardization & Data Quality	● No unified fraud detection framework across the industry. ● Data sources vary, impacting consistency in fraud detection. ● Inconsistent coding schemes and unstructured data. ● Incomplete or inaccurate claims data reduces model accuracy.	● Develop industry-wide standardized fraud detection frameworks. ● Establish clear data governance policies and data-sharing agreements. ● Implement automated data validation and anomaly detection tools.
Data Complexity	● Claims data is heterogeneous, multi-modal, and lacks standardization. ● High dimensionality and integration difficulties hinder analysis. ● Limited labeled fraud data impacts machine learning model performance.	● Use Deep Learning, graph networks, and blockchain for better data management. ● Implement real-time processing and predictive analytics for fraud detection. ● Develop self-learning AI models that improve with continuous data input.
Computational Resource Constraints	● Constraints due to algorithm complexity, data size, and model architecture ● Resource constraints like memory usage, CPU, execution time, and scalability	● Use appropriate ML techniques to reduce data size using data reduction technologies and select optimal model. ● Reduce data dimensionality using PCA or feature selection, Model Pruning, parallel processing, CPU speed acceleration, and Hyperparameter Optimization
AI & ML Implementation Challenges	● Legal and privacy constraints restrict access to large datasets. ● AI models require frequent updates to address evolving fraud tactics. ● Integration with infrastructure and healthcare legacy IT systems is difficult.	● Develop privacy-preserving AI techniques such as federated learning. ● Invest in AI-compatible infrastructure and hybrid AI-legacy integration solutions. ● Implement adaptive AI models that update dynamically based on fraud trends.
Security, Privacy & Ethical Concerns	● Compliance with HIPAA/GDPR and other regulations limits fraud detection efforts. ● Maintaining patient data confidentiality while analyzing fraud is challenging. ● AI-driven fraud detection raises concerns about fairness, bias, and transparency.	● Use data anonymization, differential privacy, and blockchain for secure fraud detection that complies with regulations. ● Develop explainable AI models to ensure transparency and accountability. ● Establish ethical AI guidelines to prevent biases in fraud detection systems.
Evolving Fraud Strategies	● Fraudsters continuously adapt tactics (e.g., upcoding, phantom billing). ● Rule-based fraud detection systems struggle to keep up with new fraud patterns.	● Deploy AI-driven fraud intelligence to identify emerging fraud schemes. ● Implement real-time anomaly detection and self-learning fraud prevention models.

Table 2. (*Continued*).

Category	Gaps & Challenges	Future Directions
Data Sharing & Collaboration	● Healthcare institutions hesitate to exchange fraud-related data due to privacy concerns. ● Overwhelming fraud alerts with excessive false positives reduce efficiency.	● Establish secure data-sharing agreements while maintaining compliance. ● Improve fraud alert systems with intelligent filtering and risk prioritization mechanisms.
Government & Law Enforcement Measures	● Weak enforcement and penalties for fraud cases. ● Limited public awareness of healthcare fraud consequences.	● Strengthen fraud-related regulations and impose stricter penalties. ● Conduct awareness campaigns and fraud prevention training for healthcare providers.

7. Conclusions

This literature review examined how machine learning works to identify healthcare provider fraud. Many supervised, unsupervised, and hybrid models are discussed in these publications. Recent research has emphasized the efficiency of Deep Learning methods like Artificial Neural Networks and supervised learning models like decision trees and Random Forests in examining intricate datasets to find irregularities suggestive of fraud. The study shows that Deep Learning techniques, ensemble models, and graph network models outperform conventional machine learning models in terms of accuracy and precision. Advances in blockchain technology improve prediction capabilities and increase the security and privacy of personal data. Comprehensive analysis shows that rules-based, anomaly, graph-based network, and blockchain technology models may produce false positives, even though hybrid models can improve accuracy.

According to the findings of numerous studies on healthcare fraud detection, fraud activities don't always follow a predetermined pattern; rather, they have unique characteristics that make it difficult to detect them using manual criteria. The connections between different healthcare data entities must be considered in the analysis. It can be challenging to integrate data from multiple sources with different standards, privacy concerns, and data quality difficulties, although machine learning offers numerous advantages for analyzing and spotting unusual trends in medical claims. Future studies should concentrate on creating benchmark datasets, urging authorities to release the findings of fraud investigations, and improving the transparency of data preparation to improve comparability and accessibility.

The main areas of future research are anticipated to include explainable AI, blockchain-based fraud prevention, and privacy-preserving machine learning methods to improve fraud detection frameworks. To detect fraud in its early stages, increase public awareness, and educate providers, patients, insurance companies, physicians, providers, and law enforcement should collaborate. Self-learning fraud prevention models and real-time anomaly detection are required since fraud patterns are always changing. Creating AI methods that protect privacy will be one way to solve security and privacy issues. It is crucial to establish ethical AI rules to prevent biases in fraud detection systems.

Conflict of interest: The authors declare no conflict of interest.

References

1. NHCAA. The Challenge of Health Care Fraud. Available online: https://www.nhcaa.org/tools-insights/about-health-care-fraud/the-challenge-of-health-care-fraud (accessed on 5 March 2025).
2. The Office of Public Affairs. National Health Care Fraud Enforcement Action Results in 193 Defendants Charged and Over $2.75 Billion in False Claims. Available online: https://www.justice.gov/archives/opa/pr/national-health-care-fraud-enforcement-action-results-193-defendants-charged-and-over-275-0 (accessed on 5 March 2025).
3. Kelly JE. 2023 Health Care Fraud and Abuse Control Program Report Reveals $3.4 Billion in Fraud Recovery. Available online: https://natlawreview.com/article/2023-health-care-fraud-and-abuse-control-program-report-reveals-34-billion-fraud (accessed on 5 March 2025).
4. United States Sentencing Commission. Health Care Fraud. Available online: https://www.ussc.gov/research/quick-facts/health-care-fraud (accessed on 5 March 2025).
5. Oversight.gov. Medicaid Fraud Control Units Fiscal Year 2023 Annual Report. Available online: https://www.oversight.gov/sites/default/files/documents/reports/2024-10/OEI-09-24-00200-1.pdf (accessed on 5 March 2025).
6. GAO Highlights. Medicare and Medicaid Additional Actions Needed to Enhance Program Integrity and Save Billions. Available online: https://www.gao.gov/assets/gao-24-107487-highlights.pdf (accessed on 5 March 2025).
7. Al Hosani M, Aljaberi SS, Nobanee H. Academic Trends in Insurance Fraud Research. SSRN Electronic Journal. 2024. doi: 10.2139/ssrn.4978584
8. du Preez A, Bhattacharya S, Beling P, et al. Fraud detection in healthcare claims using machine learning: A systematic review. Artificial Intelligence in Medicine. 2025; 160: 103061. doi: 10.1016/j.artmed.2024.103061
9. Ali O, Abdelbaki W, Shrestha A, et al. A systematic literature review of artificial intelligence in the healthcare sector: Benefits, challenges, methodologies, and functionalities. Journal of Innovation & Knowledge. 2023; 8(1): 100333. doi: 10.1016/j.jik.2023.100333
10. Iqbal MS, Abd-Alrazaq A, Househ M. Artificial Intelligence Solutions to Detect Fraud in Healthcare Settings: A Scoping Review. Advances in Informatics, Management and Technology in Healthcare; 2022. doi: 10.3233/shti220649
11. Guntoro AS, Arifin S, Noor MS, et al. Fraud in The Implementation of the Health Insurance Program: A Systematic Literature Review. Pakistan Journal of Life and Social Sciences (PJLSS). 2024; 22(1). doi: 10.57239/pjlss-2024-22.1.00315
12. Gandhar A, Gupta K, Pandey AK, et al. Fraud Detection Using Machine Learning and Deep Learning. SN Computer Science. 2024; 5(5). doi: 10.1007/s42979-024-02772-x
13. Mazumder MSA, Rahman MA, Chakraborty D. Patient Care and Financial Integrity in Healthcare Billing Through Advanced Fraud Detection Systems. Academic Journal on Business Administration, Innovation & Sustainability. 2024; 4(2): 82-93. doi: 10.69593/ajbais.v4i2.74
14. Guo Y. Application of Machine Learning in Insurance Fraud Detection: Achievements and Future Prospects. Advances in Intelligent Systems Research; 2024. doi: 10.2991/978-94-6463-512-6_65
15. Nabrawi E, Alanazi A. Fraud Detection in Healthcare Insurance Claims Using Machine Learning. Risks. 2023; 11(9): 160. doi: 10.3390/risks11090160
16. Odufisan OI, Abhulimen OV, Ogunti EO. Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria. Journal of Economic Criminology. 2025; 7: 100127. doi: 10.1016/j.jeconc.2025.100127
17. Azad T, William P. Fraud detection in healthcare billing and claims. International Journal of Science and Research Archive. 2024; 13(2): 3376-3395. doi: 10.30574/ijsra.2024.13.2.2606
18. Sayem MA, Taslima N, Sidhu SG, et al. A quantitative analysis of healthcare fraud and utilization of ai for mitigation. International journal of business and management sciences. 2024; 4(7): 13-36. doi: 10.55640/ijbms-04-07-03
19. Hamid Z, Khalique F, Mahmood S, et al. Healthcare insurance fraud detection using data mining. BMC Medical Informatics and Decision Making. 2024; 24(1). doi: 10.1186/s12911-024-02512-4
20. Parshuram HP, Joshi SG. A Comprehensive Analysis of Provider Fraud Detection through Machine Learning. International Journal of Advanced Research in Science, Communication and Technology. 2023; 3(2): 139-149. doi: 10.48175/ijarsct-14217
21. Settipalli L, Gangadharan GR. WMTDBC: An unsupervised multivariate analysis model for fraud detection in health insurance claims. Expert Systems with Applications. 2023; 215: 119259. doi: 10.1016/j.eswa.2022.119259

22. Sharma C, Vaid A, Kumar Saini M. Artificial Intelligence Driven Fraud Detection in SAP for Retail and Healthcare. International Journal of Science and Research (IJSR). 2024; 13(11): 312-315. doi: 10.21275/sr24119111713
23. Lekkala LR. Importance of Machine Learning Models in Healthcare Fraud Detection. Voice of the Publisher. 2023; 9(4): 207-215. doi: 10.4236/vp.2023.94017
24. Das S, Krishna Bhat A. Leveraging Artificial Intelligence for Early Fraud Detection in Insurance: Focusing on Intake and Claims Processing. International Journal of Science and Research (IJSR). 2024; 13(11): 1121-1124. doi: 10.21275/sr241119105452
25. Shungube PS, Bokaba T, Ndayizigamiye P, et al. A Deep Learning Approach for Healthcare Insurance Fraud Detection. Research Square; 2024. doi: 10.21203/rs.3.rs-5453482/v1
26. De Meulemeester H, De Smet F, van Dorst J, et al. Explainable unsupervised anomaly detection for healthcare insurance data. BMC Medical Informatics and Decision Making. 2025; 25(1). doi: 10.1186/s12911-024-02823-6
27. Mayaki MZA, Riveill M. Multiple Inputs Neural Networks for Fraud Detection. In: Proceedings of the 2022 International Conference on Machine Learning, Control, and Robotics (MLCR); 2022. doi: 10.1109/mlcr57210.2022.00011
28. Fursov I, Kovtun E, Rivera-Castro R, et al. Sequence Embeddings Help Detect Insurance Fraud. IEEE Access. 2022; 10: 32060-32074. doi: 10.1109/access.2022.3149480
29. Dey R, Roy A, Akter J, et al. AI-Driven Machine Learning for Fraud Detection and Risk Management in U.S. Healthcare Billing and Insurance. Journal of Computer Science and Technology Studies. 2025; 7(1): 188-198. doi: 10.32996/jcsts.2025.7.1.14
30. Devaguptam S, Gorti SS, Akshaya TL, et al. Automated Health Insurance Processing Framework with Intelligent Fraud Detection, Risk Classification and Premium Prediction. SN Computer Science. 2024; 5(5). doi: 10.1007/s42979-024-02801-9
31. Johnson JM, Khoshgoftaar TM. Data-Centric AI for Healthcare Fraud Detection. SN Computer Science. 2023; 4(4). doi: 10.1007/s42979-023-01809-x
32. Chirchi KE, Kavya B. Unraveling Patterns in Healthcare Fraud through Comprehensive Analysis. In: Proceedings of the 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom); 2024. doi: 10.23919/indiacom61295.2024.10498727
33. Narne H. Machine Learning for Health Insurance Fraud Detection: Techniques, Insights, and Implementation Strategies. International Journal of Research and Analytical Reviews. 2024.
34. Hancock JT, Bauder RA, Wang H, et al. Explainable machine learning models for Medicare fraud detection. Journal of Big Data. 2023; 10(1). doi: 10.1186/s40537-023-00821-5
35. Islam Prova NN. Healthcare Fraud Detection Using Machine Learning. In: Proceedings of the 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI); 2024. doi: 10.1109/icoici62503.2024.10696476
36. El-Enen MAA, Tbaishat D, Sahlol AT, et al. Fraud Detection in Medical Insurance Claims Using Majority Voting of Multiple Unsupervised Algorithms. Procedia Computer Science. 2024; 244: 9-22. doi: 10.1016/j.procs.2024.10.173
37. Talukder MdA, Khalid M, Uddin MA. An integrated multistage ensemble machine learning model for fraudulent transaction detection. Journal of Big Data. 2024; 11(1). doi: 10.1186/s40537-024-00996-5
38. Wang Z, Chen X, Wu Y, et al. An Interpretable Model for Health-care Insurance Fraud Detection. Research Square; 2024. doi: 10.21203/rs.3.rs-5012877/v1
39. Yao J, Yu S, Wang C, et al. Medicare Fraud Detection Using WTBagging Algorithm. In: Proceedings of the 2021 7th International Conference on Computer and Communications (ICCC); 2021. doi: 10.1109/iccc54389.2021.9674545
40. Hancock JT, Wang H, Khoshgoftaar TM, et al. Data reduction techniques for highly imbalanced medicare Big Data. Journal of Big Data. 2024; 11(1). doi: 10.1186/s40537-023-00869-3
41. Tajrobehkar M, Guo X, Nguyen D, et al. Utilization Analysis and Fraud Detection in Medicare via Machine Learning. Cold Spring Harbor Laboratory; 2025. doi: 10.1101/2024.12.30.24319784
42. Wang Z, Chen X, Wu Y, et al. A robust and interpretable ensemble machine learning model for predicting healthcare insurance fraud. Scientific Reports. 2025; 15(1). doi: 10.1038/s41598-024-82062-x
43. Kumaraswamy N, Ekin T, Park C, et al. Using a Bayesian Belief Network to detect healthcare fraud. Expert Systems with Applications. 2024; 238: 122241. doi: 10.1016/j.eswa.2023.122241
44. Mardani S, Moradi H. Using Graph Attention Networks in Healthcare Provider Fraud Detection. IEEE Access. 2024; 12:

132786-132800. doi: 10.1109/access.2024.3425892
45. Yoo Y, Shin D, Han D, et al. Medicare fraud detection using graph neural networks. In: Proceedings of the 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET); 2022. doi: 10.1109/icecet55527.2022.9872963
46. Agarwal S. Graph-Based Social Network Analysis for Uncovering Fraudulent Patterns in Health Insurance. In: Proceedings of the 2024 IEEE 15th International Conference on Software Engineering and Service Science (ICSESS); 2024. doi: 10.1109/icsess62520.2024.10719395
47. Deprez B, Vandervorst F, Verbeke W, et al. Network analytics for insurance fraud detection: a critical case study. European Actuarial Journal. 2024; 14(3): 965-990. doi: 10.1007/s13385-024-00384-6
48. Gandra a. Optimize Fraud Detection in Health Insurance Claims by Integrating Graph Analytics and Machine Learning Models. International Journal for Multidisciplinary Research. 2024. doi: 10.36948/ijfmr.2024.v06i05.27381
49. Yoo Y, Shin J, Kyeong S. Medicare Fraud Detection Using Graph Analysis: A Comparative Study of Machine Learning and Graph Neural Networks. IEEE Access. 2023; 11: 88278-88294. doi: 10.1109/access.2023.3305962
50. Lu J, Lin K, Chen R, et al. Health insurance fraud detection by using an attributed heterogeneous information network with a hierarchical attention mechanism. BMC Medical Informatics and Decision Making. 2023; 23(1). doi: 10.1186/s12911-023-02152-0
51. Jena SK, Kumar B, Mohanty B, et al. An advanced blockchain-based hyperledger fabric solution for tracing fraudulent claims in the healthcare industry. Decision Analytics Journal. 2024; 10: 100411. doi: 10.1016/j.dajour.2024.100411
52. Kapadiya K, Ramoliya F, Gohil K, et al. Blockchain-assisted healthcare insurance fraud detection framework using ensemble learning. Computers and Electrical Engineering. 2025; 122: 109898. doi: 10.1016/j.compeleceng.2024.109898
53. Selvamuthu CM, Lavaraju B, Sundaram A. A Novel Approach of Streamlining Claims Processing and Fraud Prevention in Health Insurance through Blockchain Technology. In: Proceedings of the 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC); 2024. doi: 10.1109/i-smac61858.2024.10714863
54. Guerar M, Migliardi M, Russo E, et al. SSI-MedRx: A Fraud-Resilient Healthcare System based on Blockchain and SSI. TechRxiv; 2024. doi: 10.36227/techrxiv.172055493.30957383/v1
55. Gupta G, Mandal BK, Dwivedi V, et al. Integrating Blockchain with Machine Learning for Fraud Detection in Health Insurance Claims Management. International Journal of Intelligent Systems and Applications. 2024.
56. Shruthi K, Poornima AS, Ankitha D, et al. Healthcare Insurance Fraud Detection Powered by Blockchain and Machine Learning: An Analysis and Framework. In: Proceedings of the 2024 IEEE International Conference on Smart Power Control and Renewable Energy (ICSPCRE); 2024. doi: 10.1109/icspcre62303.2024.10675307
57. Mani C, Ajay C, Harish J, et al. Block chain and AI-empowered healthcare insurance fraud detection: An analysis, architecture and future prospects. Challenges in Information, Communication and Computing Technology; 2024. doi: 10.1201/9781003559092-72
58. Samara B. Using Binary Logistic Regression to Detect Health Insurance Fraud. Pakistan Journal of Life and Social Sciences. 2024. doi: 10.57239/PJLSS-2024-22.2.00848.
59. Duman E. Implementation of Xgboost Method for Healthcare Fraud Detection. DergiPark (Istanbul University); 2022.
60. Surjuse A, Deshmukh S. Securing Healthcare Finances: AI Approach to Insurance Fraud Detection. Computer Research and Development; 2024.
61. Kumaraswamy N, Markey MK, Ekin T, et al. Healthcare Fraud Data Mining Methods: A Look Back and Look Ahead. PubMed; 2022.
62. Halimeh A. Integrating information quality in visual analytics [PhD thesis]. University of Arkansas; 2011
63. Arafat MS, Desai K, et al. Cybersecurity Challenges in Healthcare IT: Business Strategies for Mitigating Data Breaches and Enhancing Patient Trust. The American Journal of Engineering and Technology. 2025; 07(05): 15-38. doi: 10.37547/tajet/volume07issue05-03
64. Jillo G. Advances and Challenges in Fraud Detection in Medical Insurance. Available online: https://ssrn.com/abstract=4907327 (accessed on 5 March 2025).
65. Zitouni I, Postema J, van Es R. Explainable AI in fraud detection. Available online: https://www.milliman.com/en/insight/explainable-ai-in-fraud-detection (accessed on 5 March 2025).

Appendix

Table A1. Acronyms used in the study and their definitions.

Acronym	Definition
ACA	Affordable Care Act
AI	Artificial Intelligence
ANN	Artificial Neural Network
APPI	Act on the Protection of Personal Information
AUC-ROC	Area Under the Receiver Operating Characteristic Curve
AUPRC	Area Under the Precision-Recall Curve
Bagging	Bootstrap Aggregating
BBN	Bayesian Belief Network
CatBoost	Categorical Boosting
CMS	Center for Medicare and Medicaid Services
CNN	Convolutional Neural Network
DOJ	Department of Justice
DT	Decision Tree
EBC	Ensemble Bagging Classifier
EIC	Ensemble Independent Classifier
EMC	Ensemble ML Classifier
EU	European Union
FN	False Negative
FP	False Positive
GBM	Gradient Boosting Machine
GDPR	General Data Protection Regulation
GNN	Graph Neural Networks
GraphSAGE	Graph Sample and Aggregation
HCFAC	Health Care Fraud and Abuse Control Program
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
IEEE	Institute of Electrical and Electronics Engineers
IMEML	Integrated Multistage Ensemble Machine Learning
KNN	K-Nearest Neighbors
LDA	Linear Discriminant Analysis
LEIE	List of Excluded Individuals/Entities
LightGBM	Light Gradient-Boosting Machine
LIME	Local Interpretable Model-Agnostic Explanations
LR	Logistic Regression
LSTM	Long Short-Term Memory Networks
MHAMFD	Multilevel attention mechanism-based model
ML	Machine Learning
NHCAA	National Health Care Anti-Fraud Association
NIST	National Institute of Standards and Technology

Table A1. (*Continued*).

Acronym	Definition
NLP	Natural Language Processing
OIG	Office of Inspector General
PCS	Personal Care Services
PDP	Partial Dependence Plots
RF	Random Forest
RNN	Recurrent Neural Network
ROC	Receiver Operating Characteristic
SAP	Systems, Applications, and Products in Data Processing
SFS	Sequential Forward Selection
SHAP	SHapley Additive exPlanations
SMOTE	Synthetic Minority Oversampling Technique
SNA	Social Network Analysis
SSI	Self-Sovereign Identity
SVM	Support Vector Machine
TN	True Negative
TNR	True Negative Rate
TP	True Positive
TPR	True Positive Rate
WMT	Weighted MultiTree
XAI	Explainable Artificial Intelligence
XGBoost	Extreme Gradient Boosting

Table A2. Keywords used in the study and their definitions.

Keyword	Definition
Artificial Intelligence	Artificial intelligence (AI) is a field of computer science dealing with developing machines that are capable of carrying out tasks that normally call for human intelligence. Learning, thinking, solving problems, comprehending language, identifying patterns, and making decisions are some of these tasks.
Machine Learning (ML)	Machine learning (ML) is a branch of artificial intelligence (AI) that enables machines to learn automatically from data and prior experiences in order to recognize patterns and anticipate outcomes with little assistance from humans.
Supervised Learning	Supervised learning is a machine learning technique in which a labeled dataset is used to train the model.
Unsupervised Learning	Unsupervised learning is machine learning technique where model is trained using data without labeled outputs.
Healthcare Fraud Terms	
Unbundling	Making several separate billing codes for the same medical service in order to charge more than the proper bundled rate.
Upcoding	Using billing codes to obtain greater compensation for more costly services or procedures than were actually rendered.
Double billing	Charging for the same treatment or service more than once, whether on purpose or accidentally.
Kickbacks	Incentives or payments made in return for recommendations or services, which are generally prohibited in the medical field.

Table A2. (*Continued*).

Keyword	Definition
Important Measures in Machine Learning Models	
Accuracy	The capacity of the model to produce accurate predictions is referred to as accuracy. It is computed as the proportion of accurate predictions to all predictions.
Precision	Indicates how many of the positive predictions made by the model are actually correct.
Recall	The number of true positives divided by the total number of genuine positive events (true positives plus false negatives).
Specificity	Measures how many of the actual negative instances the model correctly identified.
F1 Score	A measure of a classification model's effectiveness, especially when working with unbalanced datasets
Area Under the Curve	Represents the degree of separability between classes by plotting the True Positive Rate (Recall) against the False Positive Rate (1 - Specificity). AUC value closer to 1 indicates better the model's performance.
Geometric Mean (G- mean)	A measure of how well the majority and minority classes' classification performances are balanced. Even when the negative cases are correctly categorized as such, a low G-Mean indicates poor performance in the categorization of the positive cases.
Kappa Values	A metric that illustrates the difference in performance between your classifier and a classifier that makes random guesses based on the frequency of each class.
Other Key Terms	
Conventional Machine Learning	Machine learning algorithms that use explicitly programmed rules and models to find patterns and make judgments or predictions.
Deep Learning	Deep Learning is a subset of machine learning that analyzes data using multi-layered Artificial Neural Networks.
Ensemble Modelling	It involves combining many machine learning models to enhance overall prediction accuracy.
Graph/ Network Analysis	This method uses relationships between data points structured as nodes and edges.
Blockchain Technologies	Blockchain is a decentralized digital ledger that safely keeps information on a network of computers in an unchangeable, transparent, and tamper-proof manner.