Volume (1) No (7), 2025
Journal of Global Research in Multidisciplinary Studies (JGRMS)
Review Paper/Research Paper
Available online at https://saanvipublications.com/journals/index.php/jgrms/index

Machine Learning for Medical Billing Fraud and Insurance Risk Detection: Trends and Challenges in the US Healthcare System

Dr. Bal Krishna Sharma
Professor
Department of Computer Sciences and Applications
Mandsaur University
Mandsaur
bksharma7426@gmail.com

***Abstract*—The monetary costs of healthcare fraud in the United States surpass billions of dollars annually, and to address and prevent fraud and insurance risk loss, effective data-driven methods of fraud detection and risk mitigation are required. The paper examines how Machine Learning (ML) and Artificial Intelligence (AI) hold the potential to transform current challenges. Marketable fraudulent billing practices and using ML models to improve premium risk scoring through the discovery of non-intuitive patterns in large-scale healthcare data is achievable by the means of employing supervised, unsupervised, and reinforcement learning. Recent developments are discussed and compared in various detection frameworks, and specifically, the involvement in the new technologies, Blockchain to secure data sharing and biometrics to identify. The researchers stress that scalable and explainable ML models that are consistent with the changing trends of frauds and healthcare demands are vital. In addition, it recommends cooperation between technology developers, insurers, and policymakers in order to gain ethical use of AI and adherence to data privacy policies. The results demonstrate the importance of AI as a way of improving the efficiency of the operations, financial stability, and individual care in terms of service delivery to healthcare insurance systems.**

Keywords—Machine Learning, Healthcare Fraud Detection, Insurance Risk Analysis, Medical Billing, Predictive Analytics.

I. INTRODUCTION

Healthcare remains a paramount socio-political concern in the United States, which is always listed as one of the three most important issues on the minds of voters. The American healthcare system is based on a mixed public-private model, where both people and companies may obtain health insurance with the help of a private organization, like Blue Cross Blue Shield or Kaiser Permanente, though they may receive treatment within such publicly funded institutions as the Department of Veterans Affairs, Medicare, and Medicaid [1]. This system compares so drastically with other several post-industrial countries that utilize models of universal healthcare, where all and everyone is fully covered by healthcare regardless of their socio-economic background, occupation, or health status.

The health insurance is a major industry in the establishment of care access and protection against medical emergencies. Nevertheless, fraud in the industry is becoming a problem as it erodes a sense of trust, increases overheads and prevents the provision of services [2][3]. Medical billing fraud forms part of the fraud in healthcare insurance and includes upcoding, phantom billing, duplicate claims and misrepresentation of services. Insurance companies lose billions of dollars annually due to fraud, which in turn causes premium increases, operational inefficiencies, and subpar customer service.

Healthcare billing and insurance fraud in the United States has become a serious financial and operating issue costing the healthcare system billions of dollars annually at present [4][5]. The conventional systems of fraud detection that are based on manual audit and rule-based fraud detection have failed to detect advanced fraudulent mechanism. As healthcare data is complex, high-volume and high-dimensional, standard rule-based fraud detection systems are not sufficient. They are hard to keep up with the changing practices of fraudsters, produce lots of false positives, and have to be tuned manually [6]. In response. Besides, a paradigm shift in healthcare insurance industry is under on-going as it is transforming into dynamic risk assessment. Typically, health insurance is underwritten using snapshot-based data at the time the policy is started, medical history, questionnaire, and demographics [7][8]. This methodology does not show the depth and promptness to indicate real-time changes in the health status of the insured [9]. Insurance policies may be made more individualized and flexible by utilizing the continuous data streams made possible by wearable technology, electronic health records (EHRs), and telemedicine.

The area around healthcare and insurance is changing as the world's sectors are progressively using machine learning (ML) and artificial intelligence (AI). Deep learning (DL), ensemble models, decision trees, and support vector machines (SVM) are ML approaches that are increasingly being utilized to uncover hidden patterns, perform predictive analysis, and optimize decision-making. Unguided instruction. Without labelled data, unsupervised learning methods such as clustering and anomaly detection may identify dubious assertions [10][11]. In contrast, the supervised learning methods can be applied to learn on historical fraud and then properly classify future claims. Besides the detection of frauds, ML models are currently used to insure risk scoring where they assess the customer profile to determine the likelihood of a future claim [12]. Such knowledge can assist insurers to develop superior risk management plans, minimize claim liability, and offer price-competitive models. Additionally, processing of unstructured claim notes, medical transcripts and customer complaints with Natural Language Processing (NLP) introduces the third dimension to the fraud detection and risk assessment processes

A. *Structure of the Paper*

The structure of the paper is as follows: Section I introduces the topic. Section II explains healthcare billing fraud and ML detection methods. Section III describes ML in medical insurance risk analysis. Section IV highlights Challenges and trends in healthcare. Section V reviews related literature. Section VI concludes the paper and suggests future work.

II. Healthcare Billing Fraud Using Machine Learning

Healthcare fraud is a widespread and expensive problem that compromises the effectiveness, accessibility, and quality of healthcare systems worldwide. This challenge encompasses a wide range of illegal activities, such as charging for services that were never rendered, upcoding procedures, and falsifying patient information [13].

A. *Types of Billing Fraud*

The goal of intentional deception in the healthcare industry is to get unapproved advantages. In contrast to errors and harassment, fraudulent Behavior is often classified as a criminal offence. Nevertheless, there is no universally accepted definition of fraud and abuse in health care or health insurance plans [14]. There are different types of healthcare billing fraud as show in Figure 1.

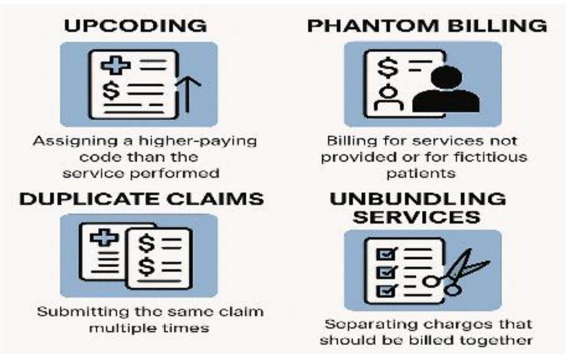

Fig. 1. Types of billing fraud in healthcare

- **Upcoding:** Upcoding is the practice of giving a service a higher-paying billing code than was actually rendered. For instance, a provider can charge for a thorough consultation even if it was just a simple visit. This dishonest technique greatly increases healthcare systems' financial losses by inflating payment amounts
- **Phantom Billing:** Phantom billing involves filing claims for services that were never provided or for patients who were never there [15]. In one instance, a group of clinicians fraudulently received millions of dollars in payments for physical therapy sessions that patients never attended.
- **Duplicate Claims:** The occurrence of duplicate claims happens when a provider files the same claim more than once, frequently with little modifications to evade automatic detection. A clinic may, for example, resubmit claims for a patient's routine checkup using slightly different coding formats in order to get many reimbursements.
- **Unbundling:** Unbundling is the process of generating distinct claims for goods or services that belong in a group. Unbundling is a distinct type of fraud that is mentioned by several writers, but it may be considered a component of poor coding. These days, software like Grouper searches for unbundling and either rejects unbundled claims or "re-bundles" the claims for the combined procedure code and adjusts the price accordingly.

B. *Machine Learning Approaches for Fraud Detection*

A subfield of artificial intelligence called machine learning (ML) enables computers to learn from data and get better over time without explicit programming. ML algorithms can examine enormous volumes of claims, patient data, and provider information in healthcare fraud detection in order to spot unusual trends and patterns that can point to fraudulent activity. There are various approaches in ML for fraud detection shown in Figure 2 and Table I.

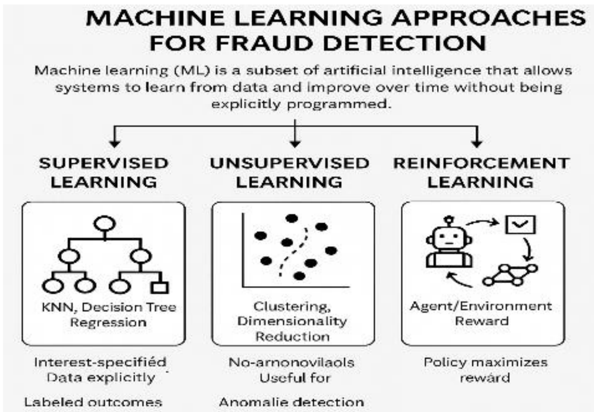

Fig. 2. Different types of machine learning approaches

1) *Supervised Learning*

Data is clearly labelled for the result, and interest is defined. For instance, the result may be the existence or non-existence of a condition such as diabetes or high blood pressure. One prerequisite for these models is that they must ensure that the result labels in the data are accurate because they are training the model on them. The performance of the developed model also be impacted by any bias in outcome assessment, which reduce the prediction's generalizability to the population outside of the dataset used to train the model. Because supervised machine learning models are used so often, the method of creating one is clearly defined and refined [16]. Some models which are used in this supervised learning like KNN, Decision Tree, Regression problems etc. the learning working shown in Figure 3.

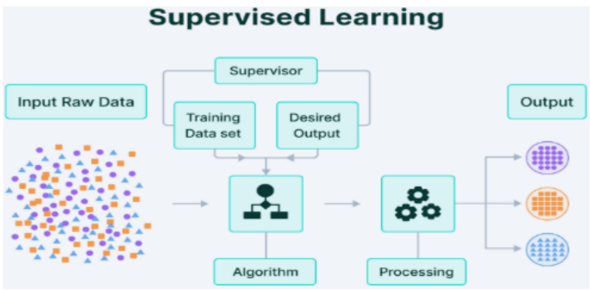

Fig. 3. Supervised Learning Approach

2) Unsupervised Learning

UL is one of the three main paradigms in ML, along-side supervised and reinforcement learning. While supervised learning relies on labelled data for training, and reinforcement learning uses approximate feedback through a reward system, UL operates in the absence of labelled outputs or feedback. Instead, it seeks to uncover underlying patterns and previously unknown knowledge within data [17][18]. Unsupervised learning is very helpful for detecting odd patterns or abnormalities in large amounts of unlabelled healthcare billing data when it comes to fraud detection. Common techniques include clustering and dimensionality reduction, which help isolate suspicious claims that deviate from normal billing behavior. This makes UL a valuable tool when labeled fraudulent cases are scarce or incomplete, and the UL approach is shown in Figure 4.

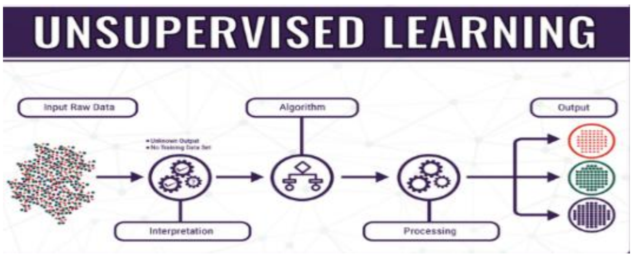

Fig. 4. Unsupervised Learning Approach

3) Reinforcement Learning

Reinforcement Learning (RL) is a ML technique that teaches agents to continuously interact with their surroundings in order to acquire decision-making functions or strategies (also known as "policy"). Inspired by human learning, this interaction consists of a series of trial and error (or "states") in which the agent receives feedback in the form of prizes for successful acts or penalties for unsuccessful ones [19]. The agent can enhance its approach and optimize anticipated cumulative rewards with the help of this input over time. The approach is shown in Figure 5.

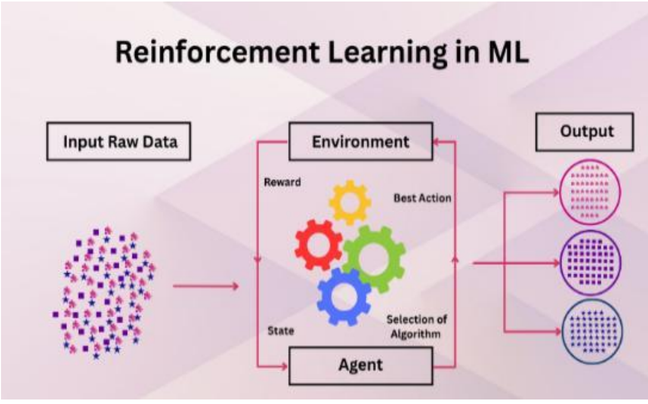

Fig. 5. Reinforcement Learning Approach

TABLE I. COMPARATIVE STUDY OF DIFFERENT TYPES OF FRAUD AND LEARNING APPROACHES

Type of Billing Fraud	Supervised Learning	Unsupervised Learning	Reinforcement Learning
Upcoding	Trains models on labeled examples of upcoded vs. correctly coded claims to classify new claims accurately.	Detects anomalies in billing amounts and codes that deviate from typical patterns.	Learns optimal policies to flag suspicious upcoding behaviors by maximizing detection rewards over time.
Phantom Billing	Identifies fake claims by comparing known legitimate service patterns with labeled fraud cases.	Clusters claim data to detect outliers (e.g., patients or services that don't exist in normal records).	Continuously learn which providers or claim patterns yield high fraud probability and improves detection rules.
Duplicate Claims	Learns from labeled duplicate claim examples to spot repeat submissions.	Detects redundant or highly similar claims through anomaly detection and similarity measures.	Adapts rules for recognizing new variations in duplicate claims through feedback/reward signals.
Unbundling	Uses labeled data to detect improper splitting of procedures/services.	Spots irregular combinations or frequent splitting patterns that differ from normal bundled billing.	Trains agents to learn optimal bundling detection policies and refine them based on reward/penalty feedback.

III. ML Approaches in Medical Insurance Risk Analysis

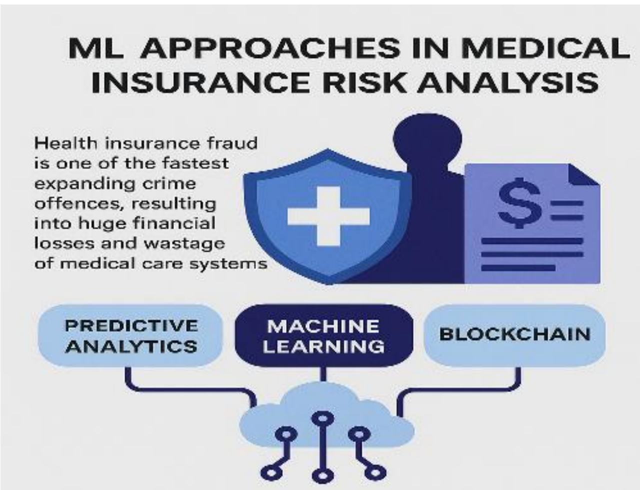

Fig. 6. Fine-Grained Resource Allocation

Health insurance fraud is one of the fastest expanding crime offences, resulting into huge financial losses and wastage of medical care systems. Flooding with ML may be necessary for some functions of fraud detection, but imposing heavy load lead to a false sense of understanding on the algorithm. It is in the context of application of AI, ML, and Blockchain in detecting fraudulent claims, that this research is conducted [20]. Using predictive analytics and security data processing, these technologies deliver increased fraud alert accuracy and prevent financial losses and guarantee the trustworthiness of the transactions of the health insurance. As the approach shown in Figure 6.

A. Role of Machine Learning in Risk Analysis

A new method for risk management, which has traditionally depended on human judgement and pre-established statistical models, is ML. By analyzing enormous amounts of data in real time, ML enables more precise and rapid risk identification than these conventional techniques.

- **Identifying risk factors:** ML techniques are increasingly being utilized to identify risk factors for adverse events in healthcare, offering a data-driven approach to enhance patient safety and clinical decision-making. Various ML algorithms and methods are, to analyze large data sets and identify complex relationships between variables. Techniques including logistic regression, decision trees, random forests, and support vector machines are employed [21][22]. These techniques enable the identification of risk factors associated with adverse events, such as medication errors, hospital-acquired infections, and patient readmissions, thereby facilitating proactive interventions and preventive measures.

- **Latency and Threshold Optimization:** Real-time fraud detection systems to function, low-latency predictions are necessary. Methods such as model compression (pruning, quantization, etc.) lower the computing burden of ML models without sacrificing precision. Operational needs, such claim numbers or the model's recent performance, are used to dynamically modify fraud detection criteria. Techniques for reinforcement learning can automate this procedure.

B. Medical Insurance Risk Detection in Machine Learning:

Health insurance fraud puts a strain on available cash and drives up healthcare costs. It is defined as "deception or intentional misrepresentation that the person or entity makes knowing that the misrepresentation could result in an unauthorized benefit for the person, entity, or another part" according to the NHACC [23]. A substantial financial concern is healthcare insurance fraud, as seen by the USD 2.6 lost for fraud recovery in 2019, stated by the US Department of Justice and the Department of Health and Human Services.

- **Dynamic Pricing Models:** Developing dynamic pricing models with real-time adaptation capabilities to individual risk profiles, regulatory changes, and shifting market conditions. To continually optimize pricing tactics, this may include combining streaming data with reinforcement learning approaches.
- **Model performance comparison:** Assessing the predictability of medical insurance rates using a variety of ML approaches, including gradient boosting, decision trees, random forests, and regression. employed stringent cross-validation and performance measures, such as R-squared, mean absolute error (MAE), and mean squared error (MSE), to assess each model's projected accuracy [24].

IV. Challenges and Trends in Health Insurance Claims

There are a few essential issues to consider when using machine learning (ML) tools to identify health insurance claim fraud. These issues are data-related, scalability, bias, and interpretability [25][26]. The two subsections below summarize the most urgent challenges to be overcome and possible mitigation plans

A. Data Privacy and Security

Healthcare data are very sensitive and therefore require compliance with privacy and security laws like HIPAA and GDPR. The information in health insurance claims is personal and contains medical information, thus open to abuse and cyber hacking.

- **Regulatory Compliance:** The ML systems have to apply encryption, anonymization, and secure storage mechanisms to legal privacy requirements.
- **Data Sharing Risks:** There is frequent collaboration between the insurers and the providers, which involves sharing of data, and the cause of concern is the risk of unauthorized access.

B. Class Imbalance in Fraudulent Data

The fraction of fraudulent claims is relatively low and modest in contrast to the overall number of claims, resulting in imbalanced datasets that bias ML algorithms.

- **Impact:** In general, models trained on skewed data may be quite accurate, but they would struggle to spot the very rare instances of false claims

C. Scalability and Real-Time Processing

Millions of claims must be processed each year by ML systems that provide real-time fraud detection.

- **Challenges:** Real-time analysis and processing of massive data volumes may be difficult for legacy infrastructure. Low-latency predictions are necessary for real-time systems to detect fraud immediately.

1) Key Issues in Healthcare

The healthcare system faces critical challenges such as unequal access, rising costs, inconsistent quality of care, workforce shortages, administrative inefficiencies, and social disparities. Addressing these issues is vital to ensure affordable, safe, and equitable healthcare for all.

- **Health Insurance Coverage:** The expense of treating patients with serious illnesses who have no insurance or inadequate income is funded by charity, increased hospital fees for people who do have insurance, or money from state, municipal, or federal taxes that are controlled by a variety of organizations [27][28]. All ultimately help to pay these expenses. Accordingly, uninsured people's medical care is not free; the costs are paid, frequently insufficiently, and the cost is split among other sources. These and other shortcomings in health care system have been discussed by me before. Providing universal health insurance to all Americans is a straightforward idea but a challenging implementation.
- **Integration with existing systems:** Examine methods for incorporating ML technologies into current healthcare systems in a seamless manner. Examine interoperability issues and suggest fixes to allow healthcare processes to effectively utilize ML findings [29].
- **Patient Safety:** To foster a culture of patient safety within hospitals, it is essential to establish an environment in which all staff members place a high priority on patient safety, actively identify and report potential dangers, and collaborate to put preventative measures into effect [30]. This is the only way to cultivate a culture of patient safety.

D. Trends of Human Healthcare System

Healthcare has evolved significantly over time from basic community care to advanced, technology-driven systems. Major milestones include the development of modern hospitals, breakthroughs in medical research, the rise of digital health, and a growing focus on patient-centered and preventive care [31]. This evolution reflects society’s ongoing efforts to improve health outcomes and adapt to changing needs.

- **Preventive Healthcare:** The fact that more and more data are becoming available due to wearable sensors and health applications is changing healthcare into a more proactive model [32]. The necessity for costly emergency procedures is being reduced by early health condition detection and chronic condition planning.
- **Personalized Medicine:** The use of genomics and AI is bringing closer the day when it is possible to customize the treatment to the genetic makeup of a person due to which the treatment becomes more effective, more precise as well as less prone to adverse effects.
- **Remote Monitoring:** The emergence of the IoT-enabled equipment is providing an opportunity to monitor patients remotely, decreasing visits to the hospital and providing continuity of care of the prevalence with chronic conditions.
- **Sustainability in Healthcare**: In search of ways to minimize their environmental practices, green technologies and sustainable practices are being implemented in hospitals and clinics around the globe, such as energy-saving buildings, waste reduction efforts.

V. Literature Review

This literature review section discusses the role of ML in medical billing fraud detection and evaluation of insurance risk. It points to AI systems that reveal the trends of frauds and help to manage risks in healthcare insurance.

Mahesh et al. (2025) found significant factors that determine insurance premiums. Generally, the results indicate that ML has great potential in predicting healthcare expenditures. Through these predictive models, insurance firms may provide more customized insurance products, simplify the underwriting process, and enable customers to make well-known decisions about their health plans [33].

Sunna et al. (2025) explored the dynamic nature of cyberattacks, the risk assessments for cyberthreats, the context of cyberattacks, and the challenges related to covering plans. It highlights how crucial AI is to evaluating cyber risks and protecting digital assets. Along with outlining the various coverage alternatives, including first-party coverage for direct costs, third-party insurance, and "silent cyber" coverage within conventional policies [34].

Váradi, Lukács and Horváth (2024) in order to assess the theoretical assumed chance of becoming an insurance fraud, a notion inspired by the response surface approach is developed. Three simply and unmistakably recognizable elements have been selected for this purpose: the insurance payout in euros, the age of the innocent participant vehicle in years; and the insurance contract's payment duration. The methodology was applied to select the parameters with the most substantial effect on the fraud risk [35].

Ahmad (2024) suggests a novel framework for preventing insurance fraud that successfully combats it by combining AI-based risk assessment with biometric identification verification. Thus, by utilizing more potent biometric identification techniques like fingerprint, face, and iris recognition in addition to machine learning algorithms to carry out dynamic risk analysis, this framework would significantly improve the accuracy and dependability of the fraud detection mechanisms. discuss the synergistic power of biometrics and AI in giving us a failsafe, instantaneous verification and risk management tool that could be adapted to the specifications of the insurance business. A thorough and methodical analysis of the suggested framework's implementation using mathematical models and computational techniques, show how it can help in detecting and averting fraudulent activities [36].

Topalov et al. (2023) investigated primary care doctors' perspectives on the use of ICT and AI in pancreatic cancer prediction, prevention, and early detection. As part of the EU-funded iHELP project, 57 primary healthcare medical specialists answered a survey on a Likert 5-scale. The findings show that while most medical professionals support the use of ICT and AI, they are not quite aware of their full potential. They are effective at identifying, extracting, and connecting important medical data in order to create trustworthy risk predictors and offer tailored prevention and intervention recommendations [37].

Dagba and Lokossou (2022) proposed a method to forecast the likelihood of health insurance premium nonpayment. The data corpus's 186 instances are divided into 127 samples (70%) for the learning phase and 59 samples (30%) for the validation and test phase. Age, marital status, whether or not a recent sickness occurred, whether or not medical spectacles or prosthesis were worn, gender, recuperation rate, and ceiling surpassed are all characteristics of each example. Following data normalization, the covariance has been calculated as part of an analysis to guarantee non-redundancy [38].

Kapadia et al. (2022) health insurance helps people pay for medical treatments in an emergency and provides financial security against the risk of debt. With health insurance and its many benefits, a number of security, privacy, and fraud issues might surface. Fraud has been a sensitive subject in the health insurance sector for a few years since it costs corporations, governments, and people a lot of money. Therefore, for both private businesses and government organizations, it is essential to build systems to detect fraudulent occurrences and payments. There is a significant amount of electronic health insurance data collected, which is extremely sensitive and draws malevolent users. Inspired by these findings, provide a comprehensive survey for safe health insurance fraud detection using blockchain technology and AI [39].

Table II summarizes recent studies on AI-based medical billing fraud detection and insurance risk analysis, effective use of ML models, and integration with technologies like biometrics and blockchain. Common limitations include data privacy concerns and model interpretability, with future work focusing on scalability, transparency, and real-world deployment.

TABLE II. Summary of Previous Study on Medical Healthcare

Reference	Study On	Approach	Key Findings	Challenges / Limitations	Future Directions
Mahesh et al. (2025)	Insurance premium prediction	Machine learning models to predict	ML can help customize insurance products, simplify underwriting.	Requires large, accurate data; model interpretability	Broader adoption of ML tools in premium

		healthcare expenditures			calculation and plan personalization
Sunna et al. (2025)	Cyber risk in insurance	Use of AI for cyber risk assessment and digital asset security	Highlights AI's role in assessing cyber threats and explains various coverage options	Evolving nature of cyber threats; gaps in traditional coverage	Develop dynamic, AI-driven cyber insurance models and address "silent cyber"
Váradi, Lukács & Horváth (2024)	Insurance fraud probability estimation	Response surface methodology with 3 key factors	Identified payout amount, vehicle age, and risk fraud	Limited to easily identifiable factors; theoretical assumptions	Expand methodology to broader datasets and real-world validation
Ahmad (2024)	Framework for preventing fraud	Assessment of AI-based biometric risks for identity verification	Biometric + AI approach enhances accuracy in fraud detection	Implementation cost; privacy concerns	Scale framework with advanced biometric tech and real-time ML models
Topalov et al. (2023)	AI for the detection and prognosis of cancer	Primary healthcare practitioners' ICT and AI use survey	Majority support ICT and AI for early detection but lack confidence	Limited trust and practical integration challenges	Improve AI tools' reliability, explainability, and user training
Dagaba & Looksee (2022)	Non-payment risk prediction	ML-based system using demographic and health variables	Demonstrated effective risk prediction using normalized, non-redundant data	Small sample size; may lack generalizability	Extend to larger datasets; refine prediction models
Kapadia et al. (2022)	Security issues in health insurance	AI-based fraud detection system with blockchain	Proposed a secure, intelligent framework with a case study	Implementation complexity; unresolved open research issues	Explore real-world deployment and integration of blockchain + AI

VI. Conclusion And Future Work

The healthcare business is ripe for fraud due to its complexity and huge monetary worth. With an ageing population comes a greater need for healthcare billing fraud prevention and optimization of insurance risk assessment. Recent developments in ML and related technologies have shown promise in these areas. Various approaches, including supervised, unsupervised, and reinforcement learning, have proven effective in analyzing large volumes of claims and patient data to identify irregularities and enhance decision-making processes. Frameworks for detecting fraud can be even more robust when these techniques are combined with blockchain technology, biometric verification, and real-time data processing. Responsible and successful application of these technologies in real-world insurance and healthcare contexts requires addressing difficulties such as data privacy, model interpretability, and practical implementation. Continued research and innovation will be crucial to adapt to emerging fraud tactics and evolving regulatory landscapes. By embracing these advanced solutions, the healthcare industry can achieve greater security, trust, and efficiency.

Future research can expand by exploring the large-scale deployment of integrated ML and blockchain systems in live healthcare insurance operations. The possibility of creating real-time premium adjustments based on continually updated risk profiles through the use of dynamic pricing models is also promising. Advancements in explainable AI (XAI) will help build trust and transparency in ML-driven fraud detection and underwriting. Additionally, further studies should focus on overcoming interoperability challenges, integrating these solutions seamlessly with existing health IT infrastructures, and ensuring compliance with evolving data security and privacy regulations.

References

[1] G. Zieff, Z. Y. Kerr, J. B. Moore, and L. Stoner, "Universal Healthcare in the United States of America: A Healthy Debate," *Medicina (B. Aires).*, vol. 56, no. 11, 2020, doi: 10.3390/medicina56110580.

[2] Z. Hamid, F. Khalique, S. Mahmood, A. Daud, A. Bukhari, and B. Alshemaimri, "Healthcare insurance fraud detection using data mining," *BMC Med. Inform. Decis. Mak.*, vol. 24, no. 1, pp. 1–24, 2024, doi: 10.1186/s12911-024-02512-4.

[3] R. Dattangire, D. Biradar, L. Dewangan, and A. Joon, "Unlocking Healthcare Fraud Detection Using Innovations of Machine Learning Strategies," in *International Conference on Data Science and Big Data Analysis*, 2025, pp. 233–249. doi: 10.1007/978-981-97-9855-1_16.

[4] R. Dey, A. Roy, J. Akter, A. Mishra, and M. Sarkar, "AI-driven machine learning for fraud detection and risk management in US healthcare billing and insurance," *J. Comput. Sci. Technol. Stud.*, vol. 7, no. 1, pp. 188–198, 2025.

[5] J. Mishra, B. B. Biswal, and N. Padhy, "Machine Learning for Fraud Detection in Banking Cyber security Performance Evaluation of Classifiers and Their Real-Time Scalability," in *2025 International Conference on Emerging Systems and Intelligent Computing (ESIC)*, IEEE, Feb. 2025, pp. 431–436. doi: 10.1109/ESIC64052.2025.10962752.

[6] S. K. Pala, "Investigating Fraud Detection in Insurance Claims using Data Science," *Int. J. Enhanc. Res. Sci. Technol. Eng.*, vol. 11, no. 3, pp. 2319–7463, 2022.

[7] B. Chaudhari and S. C. G. Verma, "Achieving High-Speed Data Consistency in Financial Microservices Platforms Using NoSQL Using Nosql (Mongodb, Redis) Technologies," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 750–759, Jun. 2024, doi: 10.48175/IJARSCT-18890.

[8] S. A. Pahune, "A Brief Overview of How AI Enables Healthcare Sector Rural Development," pp. 1–6, 2024, doi: 10.13140/RG.2.2.16675.63525.

[9] A. Pnevmatikakis, S. Kanavos, G. Matikas, K. Kostopoulou, A. Cesario, and S. Kyriazakos, "Risk Assessment for Personalized Health Insurance Based on Real-World Data," *Risks*, vol. 9, no. 3, 2021, doi: 10.3390/risks9030046.

[10] P. Goktas and A. Grzybowski, "Shaping the Future of Healthcare: Ethical Clinical Challenges and Pathways to Trustworthy AI," *J. Clin. Med.*, vol. 14, no. 5, 2025, doi: 10.3390/jcm14051605.

[11] R. Q. Majumder, "Machine Learning for Predictive Analytics: Trends and Future Directions," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 4, pp. 3557–3564, May 2025, doi: 10.38124/ijisrt/25apr1899.

[12] N. Malali, "AI Ethics in Financial Services: A Global Perspective," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 2, pp. 2456–2165, 2025, doi: /10.5281/zenodo.14881349.

[13] E. A. Makandah, E. E. Aniebonam, S. Blossom, A. Okpeseyi, and O. O. Waheed, "AI-Driven Predictive Analytics for Fraud Detection in Healthcare: Developing a Proactive Approach to Identify and Prevent Fraudulent Activities 1," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 1, pp. 1521–1529, 2025.

[14] B. Chaudhari and S. C. G. Verma, "Synergizing Generative AI and Machine Learning for Financial Credit Risk Forecasting and Code Auditing," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 11, no. 2, pp. 2882–2893, Apr. 2025, doi: 10.32628/CSEIT25112761.

[15] S. Pandya, "Predictive Modeling for Cancer Detection Based on

Machine Learning Algorithms and AI in the Healthcare Sector," *TIJER - Int. Res. J.*, vol. 11, no. 12, pp. 549–555, 2024.

[16] S. J. Wawge, "A Survey on the Identification of Credit Card Fraud Using Machine Learning with Precision, Performance, and Challenges," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 4, pp. 3345–3352, May 2025, doi: 10.38124/ijisrt/25apr1813.

[17] B. Rolf *et al.*, "A Review on Unsupervised Learning Algorithms and Applications in Supply Chain Management," *Int. J. Prod. Res.*, vol. 63, no. 5, pp. 1933–1983, Mar. 2025, doi: 10.1080/00207543.2024.2390968.

[18] S. Pahune and N. Rewatkar, "Large Language Models and Generative AI ' s Expanding Role in Healthcare Large Language Models and Generative AI ' s Expanding Role in Healthcare," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 11, no. 8, pp. 2288–2302, 2024, doi: 10.13140/RG.2.2.20109.72168.

[19] P. Jayaraman, J. Desman, M. Sabounchi, G. N. Nadkarni, and A. Sakhuja, "A Primer on Reinforcement Learning in Medicine for Clinicians," *npj Digit. Med.*, vol. 7, no. 1, 2024, doi: 10.1038/s41746-024-01316-0.

[20] G. Mantha, "Transforming the Insurance Industry with Salesforce: Enhancing Customer Engagement and Operational Efficiency," *North Am. J. Eng. Res.*, vol. 5, no. 3, 2024.

[21] A. Uttiramerur, "The Role of Machine Learning in Identifying Risk Factors for Adverse Events in Healthcare: A Comprehensive Overview," *J. Artif. Intell. Cloud Comput.*, vol. 2, no. 4, pp. 1–3, 2023, doi: 10.47363/JAICC/2023(2)205.

[22] S. Singamsetty, "Healthcare IoT Security: Examining Security Challenges and Solutions in the Internet of Medical Things. A Bibliometric Perspective," *J. Popul. Ther. Clin. Pharmacol.*, vol. 31, no. 8, pp. 1761–1806, Aug. 2024, doi: 10.53555/7j8dhs24.

[23] B. Chamarthi *et al.*, "Graph Neural Networks for Fraud Detection: Modeling Financial Transaction Networks at Scale," 2025. doi: 10.13140/RG.2.2.16907.81446.

[24] R. P. Mahajan, "Development of Predictive Models for Early Detection of Alzheimer ' s Disease Using Machine Learning," *Int. J. Curr. Eng. Technol.*, vol. 15, no. 2, pp. 115–123, 2025, doi: 10.14741/ijcet/v.15.2.3.

[25] S. Garg, "AI, Blockchain and Financial Services: Unlocking New Possibilities," *Int. J. Innov. Res. Creat. Technol.*, vol. 8, no. 1, pp. 1–4, 2022, doi: 10.5281/zenodo.15537568.

[26] N. Malali, "Artificial Intelligence in Life Insurance Underwriting: A Risk Assessment and Ethical Implications," *Int. J. Interdiscip. Res. Methods*, vol. 12, no. 1, pp. 36–49, Jan. 2025, doi: 10.37745/ijirm.14/vol12n13649.

[27] J. S. Alpert, "Twenty-First Century Health Care Challenges in the United States," *Am. J. Med.*, vol. 136, no. 7, pp. 609–610, 2023, doi: 10.1016/j.amjmed.2023.01.002.

[28] V. K. Singh, D. Pathak, and P. Gupta, "Integrating Artificial Intelligence and Machine Learning into Healthcare ERP Systems: A Framework for Oracle Cloud and Beyond," *ESP J. Eng. Technol. Adv.*, vol. 3, no. 2, pp. 171–178, 2023, doi: 10.56472/25832646/JETA-V3I6P114.

[29] S. Pandya, "Integrating Smart IoT and AI-Enhanced Systems for Predictive Diagnostics Disease in Healthcare," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 10, no. 6, pp. 2093–2105, Dec. 2024, doi: 10.32628/CSEIT2410612406.

[30] S. Mishra, "Healthcare Quality and Patient Safety: Investigate strategies for improving healthcare quality and patient safety within Indian hospitals, focusing on best practices and case studies," *Int. J. Res. Publ. Semin.*, vol. 15, no. 1, pp. 121–139, 2024.

[31] R. Q. Majumder, "A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 101–110, Apr. 2025, doi: 10.48175/IJARSCT-25619.

[32] B. K. R. Janumpally, "Securehealth: Edge-Enhanced Federated Architecture with Zero-Trust Framework for Privacy-Preserved Patient Monitoring," *Int. J. Comput. Eng. Technol.*, vol. 16, no. 1, pp. 1690–1705, 2025.

[33] M. Mahesh, B. S. Priyatham, G. SaiKumar, and K. V. V. Reddy, "Predictive Analytics for Medical Insurance Premiums," in *2025 5th International Conference on Pervasive Computing and Social Networking (ICPCSN)*, IEEE, May 2025, pp. 303–309. doi: 10.1109/ICPCSN65854.2025.11034884.

[34] A. A. Sunna, T. Sultana, N. Kshetri, and M. M. Uddin, "AssessCICA: Assessing and Mitigating Financial Losses from Cyber Attacks with Role of Cyber Insurance in Post-Pandemic Era," in *2025 13th International Symposium on Digital Forensics and Security (ISDFS)*, 2025, pp. 1–6. doi: 10.1109/ISDFS65363.2025.11012092.

[35] P. Váradi, J. Lukács, and R. Horváth, "Response Surface Methodology to Characterize the Indicators for the Early Detection of Fraudulent Cases in the Motor Insurance Market," in *2024 IEEE 11th International Conference on Computational Cybernetics and Cyber-Medical Systems (ICCC)*, 2024, pp. 201–204. doi: 10.1109/ICCC62278.2024.10582971.

[36] A. Y. A. B. Ahmad, "Fraud Prevention in Insurance: Biometric Identity Verification and AI-Based Risk Assessment," in *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*, 2024, pp. 1–6. doi: 10.1109/ICKECS61492.2024.10616613.

[37] V. Topalov, R. Kostadinov, D. Vicheva, L. Paunov, M. Georgieva, and M. Papazova, "The Primary Healthcare Providers' Attitudes towards Artificial Intelligence and Information Communication Technologies Implementation into Pancreatic Cancer Risk Prediction, Prevention and Early Diagnosis," in *2023 International Conference on Applied Mathematics & Computer Science (ICAMCS)*, IEEE, Aug. 2023, pp. 90–94. doi: 10.1109/ICAMCS59110.2023.00021.

[38] T. K. Dagba and M. F. D. Lokossou, "Neural Network For Risk Assessment In Life Insurance Industry: A Case Study," in *2022 8th International Conference on Systems and Informatics (ICSAI)*, 2022, pp. 1–4. doi: 10.1109/ICSAI57119.2022.10005386.

[39] K. Kapadiya *et al.*, "Blockchain and AI-empowered healthcare insurance fraud detection: an analysis, architecture, and future prospects," *IEEE Access*, vol. 10, pp. 79606–79627, 2022.

