AI-Driven Predictive Analytics for Fraud Detection in Healthcare: Developing a Proactive Approach to Identify and Prevent Fraudulent Activities

[1]Esther .A. Makandah; [2]Ebuka Emmanuel Aniebonam;
[3]Similoluwa Blossom Adesuwa Okpeseyi; [4]Oyindamola Ololade Waheed

[1]University of West Georgia,
Athens, Georgia, USA.

[2]Pratt School of Engineering, Duke University,
Durham North Carolina, USA.

[3]Department of Business Innovation and Strategy,
Southwest Minnesota State University,
Marshall, Minnesota, USA

[4]Department of Marketing and Supply Chain Management,
University of Oklahoma, Norman, USA

Publication Date: 2025/02/03

Abstract: The financial stability and operational effectiveness of healthcare systems around the world are threatened by the widespread problem of healthcare fraud. Conventional fraud detection systems, which rely on human investigations and retroactive audits, are unable to adequately meet the complexity and expansion of modern fraud schemes which have evolved over the years. The aim of this research is to examine the potential of AI-driven predictive analytics in preventing healthcare fraud, focusing on the development of proactive initiatives to identify and prevent healthcare-related fraudulent activities. The findings indicate that in terms of accuracy, speed, and adaptability, AI-driven predictive analytics outperforms conventional fraud detection techniques Technologies such as NLP, supervised learning, and deep learning have proven successful in revealing hidden patterns in intricate datasets. Additionally, healthcare organizations can prioritize high-risk cases and react quickly to new threats by integrating real-time fraud detection systems with risk-scoring models. Therefore, AI-driven predictive analytics can proactively support healthcare fraud detection and prevention.

Keywords: *Fraud detection, Artificial Intelligence, Predictive Analytics, Healthcare, Risk management.*

How to Cite: Esther .A. Makandah; Ebuka Emmanuel Aniebonam; Similoluwa Blossom Adesuwa Okpeseyi; Oyindamola Ololade Waheed (2025). AI-Driven Predictive Analytics for Fraud Detection in Healthcare: Developing a Proactive Approach to Identify and Prevent Fraudulent Activities. *International Journal of Innovative Science and Research Technology*, 10(1), 1521-1529. https://doi.org/10.5281/zenodo.14769423

I. INTRODUCTION

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 (Prova, 2024; Stowell et al., 2020).

According to Research and Markets (2024), the healthcare fraud analytics market is expected to develop at a compound annual growth rate of 23.6% from 2023 to 2030, from an estimated US$4.0 billion in 2023 to US$17.7 billion by 2030. This acquires vital resources from patient care while burdening insurance companies and governments. Owing to this, conventional fraud detection techniques cannot effectively address the complex rapidly evolving features of fraud schemes, which are frequently reactive and dependent on manual audits. This burden is particularly due to inadequate methods of detecting and preventing fraud, which frequently rely on manual audits and rule-based systems and are unable to keep up with increasingly complex fraudulent schemes (Nabrawi & Alanazi, 2023; Alam et al., 2024).

Artificial intelligence (AI) is an innovative technology that allows automated machines to simulate human intelligence by executing functions such as learning, reasoning, and problem-solving (Soori et al., 2023). AI systems examine enormous volumes of data, identify trends, and make informed choices using machine learning and deep learning methods. When combined with predictive analytics, AI improves the capacity to predict future events using historical data (Božić, 2023). Machine learning algorithms and statistical models are combined in AI-driven predictive analytics to produce remarkably accurate insights and predictions (Gupta et al., 2024). Therefore, this synergy can potentially transform industries by empowering organizations to predict challenges, streamline processes, and implement proactive plans in sectors including healthcare, banking, and fraud detection.

In contrast to existing rule-based systems, AI uses machine learning algorithms and advanced analytics to process enormous volumes of data and identify trends and anomalies that are potentially indicative of fraud. The ability to adjust and integrate new data guarantees that detection systems continue to be successful in combating evolving fraud strategies (Prabin Adhikari et al., 2024). Therefore, by minimizing false positives and facilitating the quick detection of high-risk transactions, AI-driven systems tend to improve accuracy. Overall, AI may reduce the operational and reputational risks associated with fraud, protect financial resources, and strengthen the assurance of organizational processes by offering proactive, scalable, and effective fraud detection solutions (Xu et al., 2024). This burden of inadequate fraud detection and prevention methods emphasizes the necessity of a proactive approach that utilizes innovative technologies like AI-driven predictive analytics. protect resources, guarantee the integrity of healthcare systems, and preserve fair access to high-quality care by enabling real-time surveillance, early identification, and prevention of fraudulent activity. Therefore, this study explores the use of AI-powered predictive analytics in healthcare fraud detection.

II. AN OVERVIEW OF HEALTHCARE FRAUD

Intentional deception or misrepresentation that leads to unapproved advantages inside the healthcare system is referred to as healthcare fraud. It is a complex problem that impacts patients, insurance companies, and the public and commercial healthcare sectors (Stowell et al., 2020). In this regard, healthcare fraud may be presented in ways such as false claims, paying for services that were never provided, duplicate claims, and prescribing needless medical treatments (Legotlo & Mutezo, 2018; Thaifur et al., 2021). These schemes, which take advantage of the complexity and size of the healthcare system, are frequently planned by people or organizations, including patients, healthcare practitioners, or organized fraud networks.

Evidence has shown that a common scheme is phantom billing, in which providers submit claims for services or equipment that are never delivered; bribery between providers and suppliers, in which financial incentives are exchanged to manipulate patient referrals or billing practices; and billing fraud, in which providers inflate charges by upcoding services or procedures to more expensive ones, such as a simple consultation being falsely billed as a specialized procedure to claim higher reimbursements (Kumaraswamy et al., 2022; Drabiak & Wolfson, 2020). However, fraud in healthcare is not limited to healthcare providers; it can also occur among patients and beneficiaries such that individuals visit several physicians to gain excess prescriptions for controlled medications, as well as identity fraud, in which an individual may obtain services using another person's insurance information (Thornton et al., 2015). These actions may potentially endanger patient safety and lead to resource misuse.

Generally, healthcare fraud has a huge financial impact however, beyond the monetary consequences, it erodes public confidence and compromises the integrity of the system. Consequently, when fraud spreads or remains unchecked (Mackey & Liang, 2012), it casts doubt on the integrity and fairness of insurance and healthcare systems (Timofeyev & Jakovljevic, 2022). In addition, patient safety may be jeopardized by dishonest tactics. Negative health effects may result, for example, from needless treatments or fake drugs that are prescribed in fraudulent schemes (Blais, 2022; UNODC 2021). A comprehensive strategy that incorporates prevention, detection, and enforcement is needed to combat healthcare fraud. The intricacy of contemporary fraud schemes is making common techniques, such as manual audits and retrospective investigations, less effective. Advanced technological solutions, particularly predictive analytics driven by AI, are becoming indispensable instruments for identifying irregularities, detecting high-risk activity, and preventing false claims even before they cause damage. Therefore, healthcare fraud requires proactive measures that utilize technology, and effective regulations to safeguard healthcare resources and guarantee fair access to quality care.

III. AI-DRIVEN PREDICTIVE ANALYTICS METHODS FOR FRAUD DETECTION

Artificial intelligence (AI) fraud detection tools use advanced computer approaches to swiftly and accurately analyze vast amounts of data, detect anomalies, and identify fraudulent trends. Machine learning (ML), in which algorithms learn from past data to identify patterns suggestive of fraud, is one of the key strategies (Devan et al., 2023; Bello & Olufemi, 2024). Unsupervised ML models are useful for identifying novel fraud schemes because they can detect outliers in datasets without previous labelling, whereas supervised ML models, which are trained on labelled datasets of fraudulent and non-fraudulent activity, can categorize and forecast suspicious transactions (Afriyie et al., 2023). A form of machine learning referred to as deep learning (DL) uses neural networks to interpret high-dimensional, complicated data, such as identifying fraudulent activity in insurance claims or electronic medical records (Nabrawi & Alanazi, 2023).

Particularly, training a model on a labelled dataset where the input data is combined with the appropriate output is considered supervised learning (Nasteski, 2017). Given that it enables the model to learn from past data and discover comparable patterns in fresh data, this method tends to be quite successful at detecting fraud. Decision trees are straightforward but effective models that base their choices on the characteristics of the incoming data by using a structure resembling a tree. In this regard, these decision trees can be used in fraud detection to evaluate different parameters, including transaction amount, location, and time, and classify transactions as either fraudulent or non-fraudulent (Afriyie et al., 2023; Gupta et al., 2017). Complex patterns in vast datasets can be learnt by neural networks, especially deep neural networks. This way, the input data is processed and transformed by several layers of interconnected nodes, or neurones. Therefore, neural networks can record non-linear correlations and interactions between features, making them especially helpful in fraud detection.

However, unlike supervised, unsupervised learning models labelled data is not necessary. Rather, they use the data's intrinsic qualities to find patterns and structures (Naeem et al., 2023). This method works well for identifying fresh and developing forms of fraud that might not have been identified before. Based on their characteristics, clustering algorithms combine related data points into groups. Clustering can be used to find groups of related transactions in fraud detection. It is possible to identify transactions that do not fit into any cluster as possible anomalies or outliers that require additional research (Ahmad et al., 2023). Algorithms for anomaly identification are made to find uncommon or uncommon patterns. For anomaly detection, methods like One-Class SVM, Isolation Forest, and k-means clustering are frequently employed (Huang et al., 2024). Therefore, because fraudulent transactions frequently display unusual behaviour in comparison to normal transactions, these algorithms are especially effective at detecting fraud.

A. Deep Learning and Natural Language Processing (NLP)

Deep Learning is a branch of machine learning that models' intricate patterns in data using multi-layered neural networks or deep neural networks. The effectiveness of deep learning approaches has been impressive across a range of applications, including fraud detection (Kumar & Manash, 2019). By considering transaction data as multi-dimensional inputs, Convolutional Neural Networks (CNNs), which are mainly used for image and geographical data analysis, can also be employed for fraud detection (Mienye & Jere, 2024). CNNs automatically extract pertinent information from the input data by using convolutional layers. CNNs can be used to examine transaction sequences and patterns over time in order to detect fraud. CNNs can identify intricate and nuanced fraud patterns that might not be seen with conventional techniques by identifying spatial links in the data. Recurrent neural networks (RNNs) are made to process time-series analysis and sequential data (Melam et al., 2024). They are appropriate for tasks involving temporal dependencies because of their capacity to retain knowledge from prior inputs (through a mechanism known as memory cells). Because they can analyze transaction histories and spot suspect patterns over time, RNNs are especially helpful in fraud detection. For example, they can identify fraudulent activities that entail a sequence of transactions over several periods, which could be a sign of sophisticated fraud schemes or money laundering. The area of AI that focuses on how computers and human language interact is called natural language processing (NLP). Textual data may be analyzed and comprehended using NLP approaches, which is useful for identifying written communication fraud. Textual data, including emails, chat conversations, and transaction descriptions, can be analyzed using NLP approaches (Mohana 2024). AI systems can detect suspicious language patterns, keywords, and phrases that can point to fraudulent intent or conduct by using text analysis (Adekunle et al., 2024; Chang et al., 2022). For instance, specific words and grammatical constructions frequently found in phishing emails may be identified as possible signs of fraud.

NLP can be employed to search for indications of social engineering, phishing, and other fraudulent techniques in emails. AI systems can identify attempts to trick users into disclosing private information or carrying out illegal activities by examining the content, structure, and context of emails (Salloum et al., 2021). Transaction descriptions can also be examined using NLP techniques to find odd or suspicious entries. For instance, transaction descriptions that contain anomalies or inconsistencies that deviate from usual trends may be marked for additional examination. Text messages, social media engagements, and customer support chats are just a few of the communication channels that may be analyzed using NLP (Bello & Olufemi, 2024; Azlaan, 2024). This therefore aids in the detection of fraudulent activity involving dishonest communication techniques.

B. *Predictive Analytics*

Across many industries, but especially in the healthcare sector, predictive analytics is innovative in detecting and preventing fraud. Healthcare organizations can examine enormous amounts of historical and current data using predictive analytics (Idemudia et al., 2024) which uses that utilizes advanced statistical algorithms and machine learning models to trace patterns and trends suggestive of fraudulent activity (Nnamdi, 2024). However, the conventional reactive fraud detection techniques, which frequently rely on manually established rules or post-fraud investigations, differ from this capability, rendering organizations susceptible to complex and evolving schemes.

Previous reports suggest that the ability of predictive analytics to detect irregularities in large databases is its main advantage (Kumari et al., 2016; Rustagi & Goel, 2022). Thus, claims and transactions in the healthcare industry are intrinsically complicated, involving a wide range of factors such as billing codes, provider practices, treatment histories, and patient demographics. These datasets can be processed by predictive analytics tools to identify departures from accepted standards (Badawy, 2023). Predictive models can identify transactions for additional scrutiny, for instance, if a healthcare provider often bills for high-value operations at a frequency that is noticeably higher than peer averages. As such, by taking a proactive stance, businesses can identify possible fraudulent activities before they cause significant financial damage.

Risk scoring is another crucial function of predictive analytics in fraud detection. Predictive models can provide risk scores to patients, providers, or claims by evaluating the probability of fraud using past data (Idemudia et al., 2024). Investigators can prioritize cases that are most likely to entail fraud by looking more closely at those with high-risk scores. This minimizes interference with valid claims and activities while simultaneously increasing the effectiveness of fraud detection efforts and lowering false positives. Furthermore, by concentrating on areas with the greatest potential impact, risk-based approaches align with organizational resources that may be constrained. By facilitating real-time transaction monitoring, predictive analytics also improves fraud detection (Mesioye & Ohiozua, 2024). Predictive algorithms can evaluate the constant streams of data produced by contemporary healthcare systems in real time to identify suspicious activity (Shukla 2023). This way, A system may, for instance, point out a patient who appears to be receiving the same care from multiple institutions or identify an unusually high number of claims from one provider over a short span. The instant alerts therefore prevent fraud from becoming worse by empowering businesses to act quickly.

The adaptability of predictive analytics and learning skills offer further advantages when integrated into fraud detection systems. A subset of predictive analytics (machine learning) allows models to change as new data becomes available, thereby increasing their accuracy. This is especially helpful in the fight against healthcare fraud since fraudsters are constantly changing their operation tactics on detection systems (Bello et al., 2023). Organizations can stay ahead of new dangers by updating predictive models to consider new fraud tendencies.

IV. APPROACHES TO IDENTIFYING AND PREVENTING HEALTHCARE-RELATED FRAUDULENT ACTIVITIES

A paradigm change from reactive detection to a prevention-focused approach is necessary to combat healthcare fraud proactively. Fraudulent schemes frequently change quickly, taking advantage of structural weaknesses and surpassing conventional safeguards. Therefore, proactive approaches focus on using innovative technologies and analytics to anticipate and prevent fraud before it happens. In addition to saving money, these methods may improve the reliability and integrity of healthcare systems. The incorporation of AI-powered predictive models, real-time fraud detection technologies, and thorough risk assessment frameworks is essential to this change.

➢ *Systems for Detecting Fraud in Real Time*

One significant development in fraud protection techniques is the use of real-time fraud detection systems (Orelaja & Adeyemi, 2024). Conventional approaches frequently depend on backward audits and investigations, which are laborious and let fraud go undiscovered until it is discovered. AI and predictive analytics-powered real-time systems examine transactions in real-time and immediately indicate questionable activity (Asghar & Abbas, 2024). For instance, a real-time system may find discrepancies between a patient's medical history and a submitted claim, or it may discover an abnormally high volume of claims filed by a single provider within a limited amount of time. Although real-time detection is instantaneous, organizations can take prompt action to stop fraudulent claims from being processed and payments from being made. Furthermore, by automating the preliminary steps of fraud detection, real-time solutions improve operational efficiency and lessen the workload for human investigators. These technologies build a dynamic defence mechanism that adjusts to the constantly shifting terrain of healthcare fraud by continuously monitoring transactions.

- *Integrating Predictive Models Driven by AI*

Predictive models driven by AI are leading the way in proactive fraud detection. To identify patterns suggestive of fraud, these models employ machine learning algorithms, historical data, and sophisticated analytics (Pan, 2024). Predictive models can identify minute anomalies that could indicate possible fraud, including billing inconsistencies or suspect provider behaviours, by being trained on databases of previous fraudulent acts. Specifically, these algorithms can identify patients who undergo duplicate treatments at several sites or clinicians who often bill for expensive procedures that are out of line with industry standards.

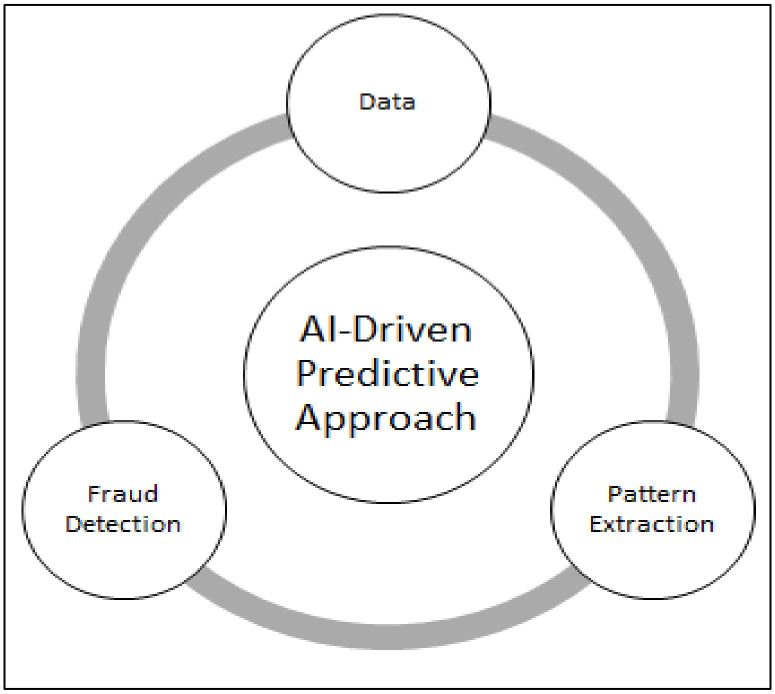

Fig 1: AI-Driven Predictive Approach for Fraud Detection

There are two benefits to incorporating these models into healthcare systems as suggested by Hilal et al., (2021). Firstly, it makes it possible to detect fraud early on, enabling businesses to take action before serious financial losses happen. Additionally, AI models are flexible enough to change with evolving fraud strategies. Machine learning algorithms can be updated and retrained when fraudsters create new techniques to keep up with new threats. A smooth, data-driven ecosystem for fraud detection and prevention can also be created by integrating predictive models with other healthcare systems, such as electronic health records (EHRs) and claims management platforms.

- *Systems for Detecting Fraud in Real Time*

One significant development in fraud protection techniques is the use of real-time fraud detection systems. Conventional approaches frequently depend on backward audits and investigations, which are laborious and let fraud go undiscovered until it is discovered. AI and predictive analytics-powered real-time systems examine transactions in real-time and immediately indicate questionable activity (Asghar & Abbas, 2024; Tariqul et al., 2024). For instance, a real-time system may find discrepancies between a patient's medical history and a submitted claim, or it may discover an abnormally high volume of claims filed by a single provider within a limited amount of time. Although real-time detection is instantaneous, organizations can take prompt action to stop fraudulent claims from being processed and payments from being made. Furthermore, by automating the preliminary steps of fraud detection, real-time solutions improve operational efficiency and lessen the workload for human investigators (Odeyemi et al., 2024). These technologies build a dynamic defence mechanism that adjusts to the constantly shifting terrain of healthcare fraud by continuously monitoring transactions.

- *Evaluation and Mitigation of Risks*

Robust risk assessment and mitigation strategies are also necessary for effective fraud prevention. Risk assessment is determining the probability of fraudulent activities in various parts of a healthcare system, which helps organizations focus on high-risk areas and prioritize resources (Pascarella et al., 2021). AI-powered analytics tools are essential in this process because they assign risk scores to providers, claims, or patient interactions based on historical data and anomalies that are detected. For instance, a provider with a history of billing inconsistencies may be assigned a high-risk score, which will cause their future claims to be closely examined.

Implementing safeguards to reduce vulnerabilities is part of mitigation measures, which are based on risk assessments (Ali et al., 2024). These approaches could involve conducting frequent audits, improving provider credentialing procedures, and fortifying internal controls. Additionally, AI can help develop prediction simulations that assess the efficacy of suggested actions and model possible fraud scenarios. Businesses can lower the risk of fraud while preserving operational effectiveness by proactively identifying and fixing vulnerabilities in healthcare systems.

V. FUTURE DIRECTIONS IN FRAUD DETECTION

➢ *Improved Interoperability and Multimodal Data Integration*

Improving data interoperability and integration across healthcare systems must be the main goal of future initiatives. High-quality datasets can be accessed with ease due to developments in data standardization, blockchain technology, and safe data-sharing platforms (Haleem et al., 2021). Predictive analytics solutions will be able to provide more accurate and trustworthy insights because of these advancements (Sinha, 2024). Subsequently, the integration of multimodal data, such as text, images, and structured data will potentially be a key component of fraud detection in the future. A comprehensive picture of healthcare operations, for instance, can be obtained by integrating claims data with electronic health records, patient feedback, and social determinants of health. The accuracy of fraud detection systems will be increased by this all-encompassing strategy.

➢ *XAI, or Explainable AI*

Ensuring sure predictive models are transparent will be essential as AI plays a bigger role in fraud detection. The goal of explainable AI (XAI) is to increase the interpretability of AI systems so that interested parties may comprehend the decision-making process (Saarela & Podgorelec 2024). This will enable an easier to comply with legal standards and increase confidence in AI-driven systems.

➢ *Learning and Adaptation*

Predictive analytics systems of the next generation will emphasize ongoing learning, allowing models to change on their own when new information and fraud trends appear (Kumar & Garg, 2018; Aldoseri et al., 2024). In the face of constantly evolving threats, fraud detection systems will continue to function effectively because of reinforcement learning and adaptive algorithms.

VI. CONCLUSION

The integration of AI-powered predictive analytics offers a transformative approach to addressing this persistent issue, allowing organizations to shift from a reactive to a proactive fraud detection and prevention strategy. Healthcare systems can use AI to analyze vast datasets in real-time, identify subtle anomalies indicative of fraud, and predict emerging patterns. The adaptability and scalability of AI-driven systems ensure that fraud detection mechanisms remain robust in the face of evolving tactics. Healthcare fraud is a significant challenge that undermines financial stability, operational efficiency, and public trust in healthcare systems worldwide. As fraudulent schemes become more complex, traditional reactive measures are no longer sufficient to safeguard resources and ensure equitable access to high-quality care.

Additionally, by reducing false positives and prioritizing high-risk activities for inquiry, the integration of risk assessment frameworks and real-time monitoring improves the effectiveness and precision of fraud detection. However, healthcare organizations may experience obstacles associated with the implementation of AI-powered solutions. Therefore, to maximize and utilize these technologies, concerns about data quality, privacy, regulatory compliance, and operational integration must be resolved.

REFERENCES

[1]. Adekunle T. S., Alabi O. O., Morolake Oladayo Lawrence, Godwin Nse Ebong, Grace Oluwamayowa Ajiboye, & Temitope Abiodun Bamisaye. (2024). The Use of AI to Analyze Social Media Attacks for Predictive Analytics. *Journal of Computing Theories and Applications*, *2*(2), 169–178. https://doi.org/10.62411/jcta.10120

[2]. Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., Ayeh, S. A., & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. *Decision Analytics Journal*, *6*(100163), 100163. https://doi.org/10.1016/j.dajour.2023.100163

[3]. Ahmad, H., Kasasbeh, B., Aldabaybah, B., & Rawashdeh, E. (2023). Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS). *International Journal of Information Technology*. https://doi.org/10.1007/s41870-022-00987-w

[4]. Alam, S., Rahman, M. A., & Chakraborty, D. (2024). Patient care and financial integrity in healthcare billing through advanced fraud detection systems. *patient care and financial integrity in healthcare billing through*

advanced fraud detection systems, *4*(2), 82–93. https://doi.org/10.69593/ajbais.v4i2.74

[5]. Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2024). AI-Powered Innovation in Digital Transformation: Key Pillars and Industry Impact. *Sustainability*, *16*(5), 1790. https://doi.org/10.3390/su16051790

[6]. Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2024). Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review. *□the □Journal of Computer Information Systems*, 1–28. https://doi.org/10.1080/08874417.2024.2329985

[7]. Asghar, J., & Abbas, G. (2024). *AI and Predictive Analytics: A New Era of Fraud Detection and AML in Financial Services*. https://doi.org/10.13140/RG.2.2.12379.99367

[8]. Azlaan, M. (2024, May 3). *Natural Language Processing (NLP) in Fraud Detection*. https://www.researchgate.net/publication/383858793_Natural_Language_Processing_NLP_in_Fraud_Detection

[9]. Badawy, M. (2023). Healthcare predictive analytics using machine learning and deep learning techniques: a survey. *ProQuest*, *10*(40), 40. https://doi.org/10.1186/s43067-023-00108-y

[10]. Bello, A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer Science & IT Research Journal*, *5*(6), 1505–1520. https://doi.org/10.51594/csitrj.v5i6.1252

[11]. Bello, O., Folorunso, A., Ejiofor, O., Zainab Budale, F., Adebayo, K., Olayemi, A., Babatunde, & Bello, C. (2023). Machine Learning Approaches for Enhancing Fraud Prevention in Financial Transactions. *International Journal of Management Technology*, *10*(1), 85–109. https://doi.org/10.37745/ijmt.2013/vol10n185109

[12]. Blais, D. (2022). *Strategies for Preventing and Mitigating Counterfeit Medication Strategies for Preventing and Mitigating Counterfeit Medication From Entering the U.S. Supply Chain From Entering the U.S. Supply Chain*. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=14481&context=dissertations

[13]. Božić V. (2023). *AI and Predictive Analytics*. https://doi.org/10.13140/RG.2.2.23798.47682

[14]. Chang, J.-W., Yen, N., & Hung, J. C. (2022). Design of a nlp-empowered finance fraud awareness model: The anti-fraud chatbot for fraud detection and fraud classification as an instance. *Journal of Ambient Intelligence and Humanized Computing*, *13*. https://doi.org/10.1007/s12652-021-03512-2

[15]. Devan, M., Prakash, S., & Jangoan, S. (2023). Predictive Maintenance in Banking: Leveraging AI for Real-Time Data Analytics. *Journal of Knowledge Learning and Science Technology*, *2*(2), 483–490. https://doi.org/10.60087/jklst.vol2.n2.p490

[16]. Drabiak, K., & Wolfson, J. (2020). What Should Health Care Organizations Do to Reduce Billing Fraud and Abuse? *AMA Journal of Ethics*, *22*(3), E221-231. https://doi.org/10.1001/amajethics.2020.221

[17]. Gupta, B., Rawat, A., Jain, A., Arora, A., & Dhami, N. (2017). Analysis of Various Decision Tree Algorithms for Classification in Data Mining. *International Journal of Computer Applications*, *163*(8), 15–19. https://doi.org/10.5120/ijca2017913660

[18]. Gupta, R., Sharma, A., & Alam, T. (2024). Building Predictive Models with Machine Learning. *Studies in Big Data*, 39–59. https://doi.org/10.1007/978-981-97-0448-4_3

[19]. Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain Technology Applications in Healthcare: An Overview. *International Journal of Intelligent Networks*, *2*(2), 130–139. https://doi.org/10.1016/j.ijin.2021.09.005

[20]. Hilal, W., Gadsden, S. A., & Yawney, J. (2021). A Review of Anomaly Detection Techniques and Applications in Financial Fraud. *Expert Systems with Applications*, *193*(1), 116429. https://doi.org/10.1016/j.eswa.2021.116429

[21]. Huang, Z., Zheng, H., Li, C., & Che, C. (2024). Application of Machine Learning-Based K-means Clustering for Financial Fraud Detection. *Academic Journal of Science and Technology*, *10*(1), 33–39. https://doi.org/10.54097/74414c90

[22]. Idemudia C., Ebele, E., & None Shadrack Obeng. (2024). Analyzing how data analytics is used in detecting and preventing fraudulent health insurance claims. *International Journal of Frontiers in Science and Technology Research*, *7*(1), 048–056. https://doi.org/10.53294/ijfstr.2024.7.1.0045

[23]. Kumar, P. R., & Manash, E. B. K. (2019). Deep learning: a branch of machine learning. *Journal of Physics: Conference Series*, *1228*, 012045. https://doi.org/10.1088/1742-6596/1228/1/012045

[24]. Kumar, V., & Garg, M. L. (2018). Predictive Analytics: A Review of Trends and Techniques. *International Journal of Computer Applications*, *182*(1), 31–37. Researchgate. https://doi.org/10.5120/ijca2018917434

[25]. Kumaraswamy N., Markey, M. K., Ekin, T., Barner, J. C., & Rascati, K. (2022). Healthcare Fraud Data Mining Methods: A Look Back and Look Ahead. *Perspectives in Health Information Management*, *19*(1), 1i. https://pmc.ncbi.nlm.nih.gov/articles/PMC9013219/

[26]. Kumari, S., Patil, Y., & Jeble, S. (2016). Role of big data and predictive analytics. *International Journal of Automation and Logistics*, *2*(4), 307. https://doi.org/10.1504/ijal.2016.10001272

[27]. Legotlo, T. G., & Mutezo, A. (2018). Understanding the types of fraud in claims to South African medical schemes. *South African Medical Journal*, *108*(4), 299. https://doi.org/10.7196/samj.2018.v108i4.12758

[28]. Mackey, T. K., & Liang, B. A. (2012). Combating healthcare corruption and fraud with improved global health governance. *BMC International Health and Human Rights*, *12*(1). https://doi.org/10.1186/1472-698x-12-23

[29]. Melam N., Reddy, C., Polavarapu Nagendra Babu, Sai, V., & Velpula Chaitanya. (2024). UPI Fraud Detection Using Convolutional Neural Networks (CNN). *Research Square (Research Square)*. https://doi.org/10.21203/rs.3.rs-4088962/v1

[30]. Mesioye, O., & Ohiozua, T. (2024). Leveraging Financial Analytics for Fraud Mitigation and Maximizing Investment Returns: A Comparative Analysis of the USA, Africa, and Nigeria. *International Journal of Research Publication and Reviews*, *5*(9), 1136–1152. https://doi.org/10.55248/gengpi.5.0924.2513

[31]. Mienye, I. D., & Jere, N. (2024). *IEEE Xplore Full-Text PDF:* Ieee.org. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10595068

[32]. Mohana M. (2024). *Natural Language Processing (NLP)*. https://doi.org/10.13140/RG.2.2.13534.04169

[33]. Nabrawi, E., & Alanazi, A. (2023). Fraud Detection in Healthcare Insurance Claims Using Machine Learning. *Risks*, *11*(9), 160. https://doi.org/10.3390/risks11090160

[34]. Naeem, S., Ali, A., Anam, S., & Ahmed, M. M. (2023). An Unsupervised Machine Learning Algorithms: Comprehensive Review. *International Journal of Computing and Digital Systems*, *13*(1), 911–921. https://doi.org/10.12785/ijcds/130172

[35]. Nasteski, V. (2017). An overview of the supervised machine learning methods. *HORIZONS.B*, *4*, 51–62. https://doi.org/10.20544/horizons.b.04.1.17.p05

[36]. Nnamdi, M. (2024). *Predictive Analytics in Healthcare*. ResearchGate; unknown. https://www.researchgate.net/publication/379478196_Predictive_Analytics_in_Healthcare

[37]. Odeyemi, O., Mhlongo, N. Z., Nwankwo, E. E., & Soyombo, O. T. (2024). Reviewing the role of AI in fraud detection and prevention in financial services. *International Journal of Science and Research Archive*, *11*(1), 2101–2110. https://doi.org/10.30574/ijsra.2024.11.1.0279

[38]. Orelaja A., & Adeyemi, A. F. (2024). *Developing Real-Time Fraud Detection and Response Mechanisms for Financial Transactions*. https://www.researchgate.net/publication/383116473_Developing_Real-Time_Fraud_Detection_and_Response_Mechanisms_for_Financial_Transactions

[39]. Pan, E. (2024). Machine Learning in Financial Transaction Fraud Detection and Prevention. *Transactions on Economics, Business and Management Research*, *5*, 243–249. https://doi.org/10.62051/16r3aa10

[40]. Pascarella, G., Rossi, M., Montella, E., Capasso, A., De Feo, G., Botti, G., Nardone, A., Montuori, P., Triassi, M., D'Auria, S., & Morabito, A. (2021). Risk Analysis in Healthcare Organizations: Methodological Framework and Critical Variables. *Risk Management and Healthcare Policy*, *Volume 14*(14), 2897–2911. Ncbi. https://doi.org/10.2147/rmhp.s309098

[41]. Prabin Adhikari, Prashamsa Hamal, & Francis Baidoo Jnr. (2024). Artificial Intelligence in fraud detection: Revolutionizing financial security. *International Journal of Science and Research Archive*, *13*(1), 1457–1472. https://doi.org/10.30574/ijsra.2024.13.1.1860

[42]. Prova N. (2024). *Healthcare Fraud Detection Using ML and AI*. https://doi.org/10.13140/RG.2.2.35327.21922

[43]. Research and Markets. (2024). *Healthcare Fraud Analytics Business Research Report 2023-2030: Growing Role of Data Mining and Pattern Recognition Spurs Innovations*. GlobeNewswire News Room; Research and Markets. https://www.globenewswire.com/news-release/2024/10/17/2965069/0/en/Healthcare-Fraud-Analytics-Business-Research-Report-2023-2030-Growing-Role-of-Data-Mining-and-Pattern-Recognition-Spurs-Innovations.html

[44]. Rustagi, M., & Goel, N. (2022). Predictive Analytics: A study of its Advantages and Applications. *IARS' International Research Journal*, *12*(01), 60–63. https://doi.org/10.51611/iars.irj.v12i01.2022.192

[45]. Saarela, M., & Podgorelec V. (2024). Recent Applications of Explainable AI (XAI): A Systematic Literature Review. *Applied Sciences*, *14*(19), 8884–8884. https://doi.org/10.3390/app14198884

[46]. Salloum, S. A., Gaber, T., Vadera, S., & Shaalan, K. (2021). Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey. *Procedia Computer Science*, *189*, 19–28.

[47]. Shukla, S. (2023). Real-time Monitoring and Predictive Analytics in Healthcare: Harnessing the Power of Data Streaming. *International Journal of Computer Applications*, *185*(8), 32–37. https://doi.org/10.5120/ijca2023922738

[48]. Sinha, R. (2024). The role and impact of new technologies on healthcare systems. *Discover Health Systems*, *3*(1). https://doi.org/10.1007/s44250-024-00163-w

[49]. Soori, M., Arezoo, B., & Dastres, R. (2023). Artificial Intelligence, Machine Learning and Deep Learning in Advanced Robotics, A Review. *Cognitive Robotics*, *3*(1), 54–70. sciencedirect. https://doi.org/10.1016/j.cogr.2023.04.001

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

[51]. Tariqul I, Islam, M., Ankur Sarkar, Rahman, O., Rakesh Paul, & Bari. (2024). Artificial Intelligence in Fraud Detection and Financial Risk Mitigation: Future

Directions and Business Applications. *International Journal for Multidisciplinary Research*, *6*(5). https://doi.org/10.36948/ijfmr.2024.v06i05.28496

[52]. Thaifur, A. Y. B. R., Maidin, M. A., Sidin, A. I., & Razak, A. (2021). How to detect healthcare fraud? "A systematic review." *Gaceta Sanitaria*, *35*(2), S441–S449. https://doi.org/10.1016/j.gaceta.2021.07.022

[53]. Thornton, D., Brinkhuis, M., Amrit, C., & Aly, R. (2015). Categorizing and Describing the Types of Fraud in Healthcare. *Procedia Computer Science*, *64*, 713–720. https://doi.org/10.1016/j.procs.2015.08.594

[54]. Timofeyev, Y., & Jakovljevic, M. (2022). Editorial: Fraud and corruption in healthcare. *Frontiers in Public Health*, *10*(1). https://doi.org/10.3389/fpubh.2022.921254

[55]. United Nations Office on Drugs and Crime . (2021). *COMBATING FALSIFIED MEDICAL PRODUCT-RELATED CR ME A GUIDE TO GOOD LEGISLATIVE PRACTICES*. United Nations Office on Drugs and Crime

[56]. Xu, J., Yang, T., Zhuang, S., Li, H., & Lu, W. (2024). AI-based financial transaction monitoring and fraud prevention with behaviour prediction. *Applied and Computational Engineering*, *67*(1), 76–82. https://doi.org/10.54254/2755-2721/67/2024ma0068