International Journal of Artificial Intelligence and Cybersecurity

https://ijaics.org/

https://ijaics.org/index.php/IJAICS/article/view/3

RESEARCH ARTICLE

AI in Healthcare Fraud Detection: Safeguarding Against Financial Crimes

Anas Bilal[1], Ahmed Shehroz[2] ,Bilal Arshad[3]

[1] University of Punjab, Lahore

[2] University of Punjab, Lahore

[3] University of Punjab, Lahore

ARTICLE INFO

Received: Nov 30, 2024
Accepted: Dec 10, 2024

Keywords
Artificial Intelligence, Healthcare Fraud, Machine Learning, Billing Fraud, Insurance Fraud, Identity Theft, Fraud Detection, Financial Crimes.

***Corresponding Author:**
anasbilal192@gmail.com

ABSTRACT

The health care sector standing as one of the largest industries in the global economy is becoming vulnerable to fraud, billing fraud, insurance fraud and identity theft. In an endeavour to reduce such risks AI technologies especially the ML algorithms are being used to identify fraudulent claims within the healthcare systems. The capability of AI in processing of data sets and interpretation of undiscoverable patterns to human beings presents a lot of benefits that can be harnessed in improving the efficiency of the detection of frauds in an organization. In this paper, the methods applied to conduct healthcare fraud with the help of AI technologies are analysed, the efficiency of their application is discussed, the threats and opportunities inherent in their implementation are identified together with ethical considerations to take into account. The implications of employing artificial intelligence in preparing the healthcare sector for future frauds will also be discussed with details of how machine learning algorithms, data and analytics, and predictive models and modelling are emerging as core tenets for protecting the industry against financial crimes.

I. INTRODUCTION

The current cases of healthcare fraud continue to manifest themselves around the world and have been proved to be expensive as they cost billions of dollars every year. This issue is not confined to geographical area or health-care system but cuts across both private and public sector systems. Some of the main cheats in healthcare consists of forged documents, misrepresentation of services, billing the wrong sum and more so, the unlawful utilization of patient data [1]. These activities erode the effectiveness of healthcare systems and organizational assets, resulting in monetary damages, increased costs of care, and, ultimately, reduced levels of patient care. The availability of a significant amount of data in the realm of healthcare has increased in

recent years and this makes it even more challenging to identify such frauds manually. In the modern world's healthcare systems, EHRs, billing, insurance data, and patient records create huge amounts of data [2].

The very volume and scope of such data present a considerable difficulty for fraud identification as conventional techniques are frequently unable to reveal subtle fraudulent transactions. In response, machine learning (ML) is rising as a very effective solution in both detecting and preventing frauds in healthcare systems. As for AI, and particularly the machine learning algorithms, it is possible to speak about their future utilization in fraud identification in the sphere of healthcare. Predictive computations can also be performed on greatly larger data sets more quickly and with greater accuracy than with M&E methods. Based on historical data and patterns that exist in fraud schemes, AI systems can highlight such activities especially in real-time application and this goes alongside the detection of fraud actions before the company incurs substantial losses [3].

Algorithms like supervised and unsupervised learning can be trained for detecting billing, claims processing, and patients' identification analyses abnormal from the norm. Supervised learning is used when there is information on the results, input in the model is given as data with previous results like fraud cases. On the other hand, unsupervised learning can discover anomalies in datasets without even having any training set and thus well suited to the detection of emerging fraud typologies. There are various forms of healthcare fraud that AI can help combat, including: Billing Fraud: This includes billing for services never provided, billing for services more than once, when they had only been delivered once and billing for a higher level of service when the actual service was of a lower level [4]. Insurance Fraud: This type of fraud involves patients or providers putting the insurance companies to the wrong side of the truth with the aim of getting an undeserving reimbursement. Identity Theft: Medical identity theft can be defined as the unauthorized use of a patient's identification data for a number of purposes that are immoral and unlawful, such as obtaining medical treatment or submitting fraudulent claims in the patient's identity. Some of the difficulties faced in adopting AI for fraud detection include However, the use of the AI technologies in identification of fraudulent activities in the healthcare sector has some issues. Data is a major question that refers to the quality and consistency of the information as well [5].

The main problem is that AI models need a huge amount of high-quality data for training, and inaccuracy of data in the field of healthcare may have negative impact on the results of AI training. Further, the social issues limiting the adoption of AI in health care; for examples privacy and bias must not be left unmentioned. In addition, due to the constant appearance of new subtypes of fraud, AI systems need to be updated regularly. As learned by the models, they are as strong as the data that feed them, and fraudsters are always innovating thus the need to constantly train and update the models [6]. In this paper, the author will focus on discussing various applications of AI and machine learning in combating healthcare fraud. First, it will describe the categories of fraud that AI can prevent, and secondly, it will consider the most popular machine learning algorithms used for fraud prevention [7].

The paper will then discuss the issues encountered in the implementation of AI based fraud detection in healthcare, such as the quality of the data used, privacy and ethical concerns. Therefore, the paper will conclude with the prospects for the application of advanced artificial intelligence in protecting healthcare organizations from financial fraud and more generally, the impact on the sector.

I. Research Findings

A. Types of AI Used in Healthcare Fraud Detection

In healthcare, there is a new trend for utilizing artificial intelligence technologies such as machine learning algorithms to detect frauds. Through working with EHR, billing data, medical insurance claims, and client records, AI may identify outliers that depict fraudulent activities. In the section below, we delve into which AI technologies are applied in healthcare fraud detection [8].

i. Machine Learning Algorithms

The major AI trend of healthcare fraud detection is machine learning. In fact, ML models are expected to identify patterns which look suspicious, and then alert security personnel once they are observed. Some of the most popular machine learning algorithms used in fraud detection include:

a. Supervised Learning:

Supervised learning, the algorithm is trained with inputs and their correct outputs and consists of a labelled set. Hence, the most common application of supervised learning in healthcare fraud detection includes activities such as Claim fraud detection, billing anomalies or discrepancies in patient records. Classification algorithms such as decision tree, random forest and support vector machines (SVM) are used often to classify a transaction as fraudulent or not [9].

ii. Decision Trees:

Decision trees work by making a number of sequential decisions on features from the data set, including but not limited to patient's age, type of treatment, and location of service. There is decision making at each node in the tree structure proposed, resulting in classification of the input data as either genuine or fake.

*a. **Random Forests**:*

Random forest constructs several decision trees, and the results of all trees are combined to enhance the model's reliability. They are particularly useful in healthcare fraud detection because they can work with large datasets that contain many features and also automatically identify rather nuanced patterns of fraudulent activity [10].

b. Unsupervised Learning:

In contrast to supervised learning, there is no need in labelled data for the implementation of the unsupervised learning algorithms. However, these algorithm process big data and make distinction on the values that differ from the set trends. For this reason, unsupervised learning is best for identifying new or previously undiscovered types of fraud that hadn't been previously identified. Some of the general types of unsupervised learning methodologies include an unsupervised clustering technique and an anomaly detection [11].

*c. **K-Means Clustering**:*

K-means clustering is an algorithm that helps to cluster data that belong into similar clusters. In healthcare fraud detection for example, this algorithm can group patient claims in different classes meaning it can detect groups with atypical behaviour that could be fraudulent.

iii. Isolation Forest:

All anomaly detection approaches for isolation forests were designed to isolate anomalies as opposed to profiling normal data points. This makes them be unique tools in detecting any anomaly in billing or any unexpected claims.

B. Deep Learning

Multi-layered artificial neural networks, a type of machine learning algorithms known as deep learning algorithms can learn from a large amount of unorganized data like medical images or large number of poorly structured notes. Deep learning is more useful for fraud detection in health care systems as most of the data sampled are usually complex and high dimensional [12].

i. Convolutional Neural Networks (CNNs)

Convolutional Neural Networks (CNNs) are one type of Deep Learning algorithm that is well-optimised for processing visually orientated data, like medical images. These are networks that are created to self-identify features from images which makes it perfect to be used in a task that involves image diagnosis such as X-rays, MRI, CT scans, and mammogram images. In healthcare fraud detection, CNN can be used to detect fraud occasioned by false claims on imaging. For example, they can sign different imaging reports, analyse changes in images submitted for compensation. When a medical imaging provider claims that an imaging procedure was conducted, or submits images that he or she manipulated to support the need for more procedures, then CNNs can help in detecting this as fraud [13]. By training CNNs on large datasets of medical imaging and their corresponding diagnoses, such networks will learn to identify markers on imaging data that smelt of fraud. CNNs make the possibility of increasing the accuracy of the fraud detection systems strengthen by automating the process of detecting any unusual characteristics that may be hard for the human reviewer to pin point.

ii. Recurrent Neural Networks (RNNs)

Recurrent Neural Networks (RNNs) are types of artificial neural network, which is capable of treating sequential data, by maintaining state from previous step of the sequence. Due to this, RNNs are well suited for tasks such as prediction for time-series, language modelling, and trending. In the area of healthcare fraud, RNNs have the potential of plotting the course of patient and their treatments and the implementation of medical procedures in the healthcare journey. For example, when comparing the history of a patient treatment the RNNs will be able to detect patterns which are peculiar and likely to entail billing inconsistencies, unauthorised changes in the patient's treatment plan or abuse of standard protocols [14]. The RNNs can also be able to recognize instances whereby treatment is prolonged where it is unnecessary or procedures are billed on multiple occasions for the same event. Analysing sequences of the records of patients and billing transactions, RNNs therefore can take step by step identification of fraudulent pattern, which might go on in an ongoing manner and might be leading across multiple stages of a patient's process of treatment.

iii. Natural Language Processing (NLP)

There is a variety of Artificial Intelligence methods, which can be applied for healthcare fraud detection, one of the most effective is a Natural Language Processing (NLP) that allows to analysis a lot of unstructured textual data like doctor's notes, patient histories or descriptions of invoices and bills. NLP can analyse text and read meaning in it and so can be used to detect anomalies or a fraud in documents [15]. There are several NLP approaches of which one refers to Named Entity Recognition (NER), that extracts specific information such as patient's name, medication, or a specific procedure. In fraud detection, NER can signal abroad pattern in the claims such as deviations in billing codes Orto Array detect lied or altered information in the medical history of the patient as presented in the claim documents. The other important NLP approach is the text classification that organizes the textual information that originates from the EHRs and insurance claims into compartments like fraud or genuine. Text classification can also identify scopes of fraud such as repetition of particular medical terms or code beneath the claim that may be indicators of upcoding for fraud claims that may not be conspicuous [16].

C. Predictive Analytics

Business intelligence entails the use of data to make future forecasts concerning an organization or business. In the scenario of healthcare fraud prevention, a type of machine learning algorithm can be used in order to predict future fraudulent occurrence based on historic defined fraud occurrences. These models are quite helpful in the instances of fraud that has not yet gone out of hand since healthcare organizations can act accordingly.

i. Regression Models:

Regression models aim to find a relationship pattern of factors (patient characteristics, medical history, or claimed types of services) to estimate the likelihood of fraud. Such models are generally applied to calculate the possibility of a given claim being fraudulent using past information [14].

*a. **Time-Series Forecasting**:*

In this case, time-series models involve analysis of past data to estimate future trend of fraudulent activities. These models assist in the identification of patterns associated with fraud and encourages the healthcare organization to direct it resources to such areas.

ii. Challenges in Implementing AI for Fraud Detection

Although AI technology has shown to work well in identifying healthcare fraud, it also has various implementation issues. These challenges can impede the successful deployment of AI technologies, requiring careful consideration of the following issues:

a. Data Quality and Availability:

Another major focus area relevant to the use of AI for fraud detection in the area of health at EMHS is the issue of data quality and accessibility. AI algorithms use large amount of high quality, standardized data to train and to generate proper prediction. Nonetheless, health care data is often incoherent, insufficient, or contradictory that lowers the efficiency of AI models [17].

b. ***Incomplete Data****:*

There might be times when there are gaps in the information in the EHRs or insurance claims and this can cause problems in how well the AI is able to determine fraud. For instance, where fields like treatment codes or patient demography are missing or contain wrong information, then the AI system may miss fraudulent compensations [18].

c. ***Data Silos****:*

Deliverables of healthcare entities are also unique as they are accumulated in various systems and data formats. This type of AI system deals with different types of data from hospital records, insurance data, and other public health data that can complicate the identification of fraud cases.

d. Privacy and Ethical Concerns:

The need to use AI in identifying healthcare fraud also leads to great privacy and ethical issues. Electronic health records include personal data so handling it with the help of AI technologies is a highly risky venture that can lead to violation of certain legal acts including HIPAA [19].

e. ***Data Privacy****:*

To this end, AI systems need to emphasize privacy and security of patients 'information. Hacking into a patient's information exposes patient's rights to invasion and attracts the rule of law.

iii. Algorithmic Bias:

The learned recommendations are only as good or bad as the data sets fed into the AI. This means that AI systems can continue to amplify existing inequities if trained on historical data with such prejudices. For instance, the developed model of an AI is trained on data from specific demographics, and therefore the AI may not identify fraud in those populations or offer wrong predictions. There is an increasing focus on fairness and bias in AI and what algorithms give to individuals, which is why it is immensely important not to allow discrimination [20].

D. Integration with Existing Healthcare Systems

The incorporation of AI technologies into healthcare has been known to be complex and expensive if integrated into ongoing health systems. Some of the realistic problems include: The AI systems disrupt the existing work routines, and this may create community's resistance from complaining that these systems will only interfere with their working schedules. Organizational users, including clinicians and administrators, may lack the willingness to implement new technologies into their practice, if the result is an increase in the technological demand for everyday work. Also, the compatibility has to be considered since AI based fraud detection systems should be integrated with current IT infrastructure, including EHR, billing software and insurance claims processing system. This often calls for considerable modifications or enhancements to present systems and optimum compatibility of AI solutions with current health systems are important for their implementation for efficient use [21].

E. Future Directions and the Role of AI in Healthcare Fraud Prevention

The effectiveness of using artificial intelligence (AI) technologies in the detection of healthcare fraud will be increasingly necessary in the future. Al has been in progress at a steady pace and its deployment will lead to further enhancements of accuracy and efficacy of the applied fraud detection systems, and to solve the problems of data quality, privacy and fairness. Just as fraud in the healthcare industry is dynamic and continues to change its methods over time, AI systems have to change as well, to accommodate new forms of fraud, and some of the innovations as described above are likely to define the future of fraud detection [20].

i. Enhanced Algorithms and Real-Time Detection

Possibly one of the most-ready for growth concerns in the future of AI fraud detection stands in the enhancement of AI algorithms, especially Deep learning and Reinforcement learning algorithms. Of the three categories of machine learning techniques, the deep learning approach shows formidable performance when dealing with a large amount of high-dimensional data, including medical images, free text, and comprehensive patient history. It helps the AI systems to find inherently complex patterns of fraud concealed by the generic and traditional methods. With deep learning's identification of known and unknown frauds, AI systems will gradually enhance the identification of genuine and fake claims in real time again, within no time. Other active fields of development, and one of the most important, are reinforcement learning that enables systems to make changes by interacting with data and adapt based on the results [22]. Such systems can always improve their models to detect the fake transactions and change their model with the updates often used by fraudsters. Real-time characteristics also improve the reliability of fraud prevention services while minimizing the research time when checking suspicious cases.

a. Integration of Blockchain Technology:

The use of the blockchain technology is viewed to significantly improve the safety and genuineness of the healthcare information and if implemented properly can significantly minimize the number of fraudulent claims. Blockchain gives a chance to have a decentralized and witness-proof register-based system, through which this or that swindler will not be able to change/falsify something. When both AI and blockchain technologies combined they can improve the accuracy and faster results of patients' records, billing data, and insurance claims [23]. The high level of secure technology that accompanies block chain guarantees that any changes that may be made on the claims or even patient details are well recorded and trackable in the event of a dispute. Such block chain data can be pam analysed through AI in order to detect something that looks out of the ordinary or a likely fraud figure. They are integrated in such a way that any opportunity which might lead to fraudulent claims is weeded out before it is processed; On the same note, the availability of accurate and comprehensive data to insurance providers and seekers, healthcare providers and patients strengthens the bond of trust which is critically important in such a business. When integrated, AI and blockchain can promote better and effective way of FD and prevention in healthcare.

b. Continuous Learning and Adaptation:

Due to the increased complexity in the types of fraud that are being developed in the future, there will be a call for continual learning of the AI-based fraud detection systems. Mainstream embezzlement check systems will always be a problem when it comes to handling new emerging fraud, whereas an AI system will be able to learn as it encounters new data. Unlike human beings, AI models are not limited to a fixed line of perception as they can always learn new aspects that make up fraudulent actions. It will enable healthcare fraud detection systems to capture new fraud

trends in real-time and make the right response. Reinforcement learning techniques will enable machines to differentiate and hone their algorithm without human interferences. This continuous adaptation is however necessary in areas such as the health care fraud detection since the fraudsters keep on developing various techniques on how best to avoid the systems put in place to detect the fraud [24]. AI systems will obtain long-lasting and easily scalable insights from new data to fight fraud and preserve vital healthcare assets. Moreover, the possibility of feedback loops will allow healthcare systems to respond to the performance of the system through ongoing updates in order to stay ahead of the particular progress of the A I systems in relation to these kinds of schemes for fraud detection. The advancements being witnessed in AI mean that the amalgamation of AI with other leadership technologies such as blockchain or the flexibility that the new environment offers will further increase the chance of identifying fraud in the healthcare industry. Subsequent developments hold the potential of decreasing the costs, increasing the level of performance, and enhancing the healthcare data security; in other words, contemporary healthcare fraud prevention research offers a stronger solution on all these points in the future.

F. Collaborative Efforts Between AI and Healthcare Stakeholders

The use of AI in detecting healthcare fraud involves all the players in the industry; the providers, the insurers, the regulators, and the technology gurus. These parties have to collectively co-ordinate themselves, in order to not only build and implement AI technologies for the detection of fraud, but also do so sustainably and in compliance with the set standards of ethics and laws regulating the practice, as well as for the practical functioning and optimization of the healthcare delivery systems. The healthcare industry will be able to develop stronger, more efficient, and equitable measures against fraud if such entities collaborate [20].

a. Multi-Party Collaboration for Effective Fraud Prevention:

Organizational prevention of fraud requires that AI systems are designed and applied in a complex model that encompasses other actors. This structure opens opportunity for multiple parties such as scientist, healthcare personnel, policy makers, insurance companies and the developers of Artificial Intelligence technologies to all come together, thus offering their individual expertise in the development of a full package of means of fighting frauds. Heath care organizations are responsible for recognizing potential fraud situations in patient records, billing and clinical procedures in healthcare delivery. Their day to day working with the patients gives them knowledge of what constitutes proper treatment and billing. But else their efforts may not be enough to flag intricate fraud especially when the fraud masks the data with competent semblances of legal tenderness. However, this is where AI can come in handy, finding those subtle issues which may be overlooked in a large dataset. Insurance companies being some of the major stakeholders have prerogative of dealing with huge volumes of claims data and fraud reports. AI systems can therefore complement fraud analysis options by involving healthcare providers in the sharing of such insights in regards to claims fraud [23]. In this paper, when information on billing patterns from insurers and the data collected from the healthcare systems is integrated into the AI models, it is easier for the models to identify an anomaly. By nature, regulators are required to define the legal requirements, codes, and best practices within which AI-based fraud detection systems should provide service. They play the role of checking whether the AI solutions meet the laws set down in the domain of healthcare including privacy and security of patient information. In addition, some regulators support the integration of the data sharing of health care providers, insures, and other stakeholders with the intent of providing structure to aid in the construction of more effective and efficient AI fraud detection models.

b. The Role of Insurers, Healthcare Providers, and Regulators in AI Adoption:

Health insurance companies, health care organizations and agencies, and regulatory authorities have key roles to encourage and enable AI based anti-fraud systems in the health care network. Insurance companies, being direct beneficiaries of the innovation, offer the historical claims data needed for training the AI models, and would benefit from the accuracy of the fraud detection. They also motivate adoption of AI by providing grant support for pilot projects and challenging healthcare organizations to incorporate AI into fraud-fighting practices while respecting the privacy requirements of patients, including HIPAA [25]. Healthcare providers, critical for the success of AI models, provide the data and understandings of the clinical practice to ensure that AI works to identify fraud while not negatively impacting patient care. They also have to prove that AI based decisions made by the algorithm are reasonable and legal as well as are within ethical and clinical norms. From the creation of frameworks for ethical application of artificial intelligence, regulators set data privacy measures, and deal with healthcare matters. They also maintain relationships with the various stakeholders and keep the AI systems operating fresh as new fraud methodologies are developed, enhance confidence in the technologies.

II. Conclusion

The employment of AI in the identification of fraud in the healthcare sector is a major improvement in fighting the rising menace of fraud in the healthcare sector. Modern artificial intelligence technologies such as machine learning, natural language processing, deep learning to help economically both protect health care resources from frauds and help patients get what they are entitled to deserve. Using claims history, imaging data, and patient files, AI learns patterns and deviations from the norm that otherwise stay unseen, thereby contributing to healthcare fraud costs' decrease. However, the efficient use of AI in healthcare fraud detection is possible only if the insurers, healthcare providers, regulators, as well as the developers of the AI technologies, work together. These stakeholders have critical parts to play on what an AI model is, how ethical it is, and whether it will meet the privacy and legal requirements. Although there are key issues, which still persist with AI adoption to prevent fraud, the prospects for AV use in fraud appear bright. Thus, given the continuous growth in innovations in AI technologies, ethical issues, and policies, AI systems will go a long way in transforming how HS prevent and avoid fraud effectively to generate increased health safety.

III. References

1. Chan, S., & Chen, D. (2020). *Artificial Intelligence in Healthcare Fraud Detection: A Systematic Review*. International Journal of Medical Informatics, 139, 104124.
2. Zhang, Y., Li, X., & Wang, Z. (2019). *Machine Learning for Healthcare Fraud Detection*. Computers in Biology and Medicine, 114, 103436.
3. UCI Machine Learning Repository (2021). *Health Insurance Fraud Detection Dataset*. Retrieved from https://archive.ics.uci.edu/ml/datasets/Health+Insurance+Fraud+Detection
4. Ramsbotham, S., Kiron, D., & Prentice, P. (2018). *Artificial Intelligence in Health: A Framework for Fraud Detection*. Harvard Business Review, 96(3), 50-59.
5. Bhat, V., & Kadaba, P. (2020). *AI-Powered Fraud Detection in Healthcare: Prospects and Challenges*. Journal of Healthcare Information Management, 34(4), 15-22.
6. Sandhu, R., & Sharma, A. (2020). *Natural Language Processing and AI for Healthcare Fraud Detection*. Journal of Medical Systems, 44(8), 134.

7. Saeed, A., Husnain, A., Zahoor, A., & Gondal, R. M. (2024). A comparative study of cat swarm algorithm for graph coloring problem: Convergence analysis and performance evaluation. International Journal of Innovative Research in Computer Science and Technology (IJIRCST), 12(4), 1-9. https://doi.org/10.55524/ijircst.2024.12.4.1
8. Ho, S. T., & Tan, C. K. (2020). *Artificial Intelligence and Big Data Analytics for Fraud Detection in Healthcare*. International Journal of Advanced Computer Science and Applications, 11(6), 107-113.
9. Nor, N. M., & Tharim, M. M. (2020). *AI-Based Systems for Healthcare Fraud Prevention: Implementation and Ethical Concerns*. Journal of Health Informatics, 26(2), 51-58.
10. Husnain, A., & Saeed, A. (2024). AI-enhanced depression detection and therapy: Analyzing the VPSYC system. IRE Journals, 8(2), 162-168. https://doi.org/IRE1706118
11. Li, L., & Xu, B. (2019). *Healthcare Fraud Detection: A Machine Learning Approach*. Journal of Healthcare Engineering, 2019, 1-10.
12. Husnain, A., Alomari, G., & Saeed, A. (2024). AI-driven integrated hardware and software solution for EEG-based detection of depression and anxiety. International Journal for Multidisciplinary Research (IJFMR), 6(3), 1-24. https://doi.org/10.30574/ijfmr.2024.v06i03.22645
13. Lee, S., & Kim, M. (2021). *Challenges and Opportunities of Implementing AI in Healthcare Fraud Prevention*. Artificial Intelligence in Healthcare, 5(3), 110-122.
14. *Chen, JJ., Husnain, A., Cheng, WW. (2024). Exploring the Trade-Off Between Performance and Cost in Facial Recognition: Deep Learning Versus Traditional Computer Vision. In: Arai, K. (eds) Intelligent Systems and Applications. IntelliSys 2023. Lecture Notes in Networks and Systems, vol 823. Springer, Cham. https://doi.org/10.1007/978-3-031-47724-9_27*
15. Williams, C., & Johnson, A. (2020). *Leveraging AI for Fraud Prevention in Healthcare: A Comparative Analysis*. International Journal of Healthcare Technology, 9(4), 92-104.
16. Kumar, S., Hasan, S. U., Shiwlani, A., Kumar, S., & Kumar, S. DEEP LEARNING APPROACHES TO MEDICAL IMAGE ANALYSIS: TRANSFORMING DIAGNOSTICS AND TREATMENT PLANNING.
17. Shiwlani, A., Khan, M., Sherani, A. M. K., & Qayyum, M. U. (2023). Synergies of AI and Smart Technology: Revolutionizing Cancer Medicine, Vaccine Development, and Patient Care. International Journal of Social, Humanities and Life Sciences, 1(1), 10-18.
18. Shiwlani, A., Ahmad, A., Umar, M., Dharejo, N., Tahir, A., & Shiwlani, S. (2024). BI-RADS Category Prediction from Mammography Images and Mammography Radiology Reports Using Deep Learning: A Systematic Review. Jurnal Ilmiah Computer Science, 3(1), 30-49.
19. Thatoi, P., Choudhary, R., Shiwlani, A., Qureshi, H. A., & Kumar, S. (2023). Natural Language Processing (NLP) in the Extraction of Clinical Information from Electronic Health Records (EHRs) for Cancer Prognosis. International Journal, 10(4), 2676-2694.
20. Shiwlani, A., Ahmad, A., Umar, M., Dharejo, N., Tahir, A., & Shiwlani, S. (2024). Analysis of Multi-modal Data Through Deep Learning Techniques to Diagnose CVDs: A Review. International Journal, 11(1), 402-420.
21. Shah, Y. A. R., Qureshi, S. M., Ahmed, H., Qureshi, S. U. R. S., Shiwlani, A., & Ahmad, A. (2024). Artificial Intelligence in Stroke Care: Enhancing Diagnostic Accuracy, Personalizing Treatment, and Addressing Implementation Challenges.
22. Khurshid, G., Abbassi, A. Z., Khalid, M. F., Gondal, M. N., Naqvi, T. A., Shah, M. M., ... & Ahmad, R. (2020). A cyanobacterial photorespiratory bypass model to enhance photosynthesis by rerouting photorespiratory pathway in C3 plants. *Scientific Reports*, *10*(1), 20879.
23. Kumar, V., & Gupta, A. (2021). *AI in Healthcare Fraud Detection: The Next Frontier in Data Security*. Journal of Health Data Science, 7(1), 42-53.

24. Patel, M., & Shukla, R. (2021). *Improving Fraud Detection in Healthcare with AI and Machine Learning Techniques*. Journal of Medical Fraud Prevention, 4(3), 25-37.
25. Choi, J. E., Qiao, Y., Kryczek, I., Yu, J., Gurkan, J., Bao, Y., ... & Chinnaiyan, A. M. (2024). PIKfyve, expressed by CD11c-positive cells, controls tumor immunity. *Nature Communications*, *15*(1), 5487.