International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.56472/ICCSAIML25-109
Eureka Vision Publication | ICCSAIML'25-Conference Proceeding

Original Article

AI in Fraud Detection: Leveraging Machine Learning to Combat Insurance Fraud

Vasanta Kumar Tarra
Lead Engineer.

Abstract - *An Increasing problem, insurance fraud causes yearly losses for businesses of billions of dollars & drives higher rates for actual policyholders. Usually based on rule-based methods that find it difficult to change with the dynamic strategies used by Scammers, traditional Scam detection systems For AI & ML, this is the Domain of intervention. By analyzing more amounts of data & exposing hidden tendencies, AI-driven Scam detection systems can find bogus claims with more speed & accuracy. ML models always improve by absorbing lessons from past events, therefore reducing false positives & identifying perhaps small-scale Misleading activity. Using methods like anomaly detection, natural language processing (NLP), & predictive analytics which help to identify misleading activity helps to improve productivity & reduce economic losses. The benefits of fraud detection motivated by AI go beyond simple financial savings. It minimizes unnecessary delays & speeds legitimate claims, therefore enhancing the user experience. As technology develops, insurance companies could expect ever more advanced solutions combining IoT, block chain, AI, and improved biometrics. Still, challenges remain including data privacy concerns & the need of openness in AI policy-making. Improving AI models & keeping their dominance against ever complex fraud schemes will depend on future research and invention. The insurance industry has to balance automation with human knowledge as AI use rises to maximize efficiency while maintaining trust and equity.*

Keywords - *Insurance fraud, machine learning, fraud detection, artificial intelligence, supervised learning, unsupervised learning, anomaly detection, predictive analytics, claims processing, fraud prevention.*

1. Introduction

An ongoing problem affecting businesses as well as policyholders is insurance fraud. From too strong assertions to completely invented events, con artists are always looking for fresh ways to control the system. Conventional cheat detection techniques based on defined criteria and hand estimations could not be sufficient to handle the increasing complexity of these systems. This not only causes Economical losses for insurance companies but also results in higher premiums for ethical customers.

ML & AI are reshining the fight against insurance fraud. By means of large-scale data analysis, hidden pattern discovery, & continuous adaptation to new Scam techniques, AI-driven solutions improve the speed, intelligence, & efficiency of fraud detection. Unlike traditional rule-based systems, AI may find subtle abnormalities that might escape human experts, therefore improving fraud detection programs greatly. Insurance Scam has serious consequences. Industry data show that bogus claims cause insurance companies to lose billions of dollars yearly & that 10% of all insurance claims are thought to be fraudulent. These losses affect not just insurance firms but also cause customers to pay more.

Demand for creative, flexible scam detection systems has never been more important as fraudsters get ever more sophisticated using digital tools & deep fake technologies to alter claims. The effect of AI & ML on insurance sector scam detection is investigated in this paper. First we will look at the several forms of insurance scam & their financial effects. We will then investigate the shortcomings of traditional scam detection methods & their causes. Finally, we will investigate how AI may prevent Scam, stressing its advantages & juxtaposing them with more conventional approaches. In the fight against scammers, AI is a transforming agent not only a tool.

2. AI and Machine Learning in Fraud Detection

The progress in insurance scam detection is no longer from rule-based systems to machine learning models but to more sophisticated models that have the power to effectively find complex scam patterns with precision. AI-powered scam detection merges supervised and unsupervised learning techniques, deep learning models, and hybrid approaches to identify suspicious claims. In addition to the learning from extensive data sets, these models increase efficiency in the detection of scam, reduce false positives, and help the insurers avoid losses.

2.1 Supervised Learning for Fraud Detection

In the field of scam detection, supervised learning is a frequently employed AI method. This method is based on a model that is trained on the labeled data that either declares the claim to be true or false. Consequently, the algorithm is taught to isolate the two, which implies its power to identify scams in the new claims.

2.1.1 Common Supervised Learning Algorithms

Several machine learning algorithms are widely used in fraud detection:

- An easy yet effective classification model used in logistic regression estimate the probability of a claim being fake. When scammer's patterns show a linear association, it works well; but, complex scam techniques coul
- A rule-based approach, decision trees divide data into branches based on several scam indicators including claim size, claimant history, & geographical location. Though they may over fit the data, decision trees are easily understood.
- Random forests are a development of decision trees using numerous trees to increase validity. Through averaging the predictions of many trees, random forests reduce over fitting and improve the accuracy of scam detection.
- Four Support Vector Machines (SVMs) are a useful tool for efficiently spotting scam trends by use of optimal boundary separating between legitimate & fraudulent claims. Although Support Vector Machines are good for complex datasets, they could have high running costs.

2.1.2 Data Labeling for Fraud Detection

To achieve supervised learning's effectiveness, accurate labeled training data is the crucial condition. Nowadays, insurers determine the past claims are fraudulent or non-fraudulent according to fraud investigation, and then model development affects. On top of that, the possibility of marking data is always there as the occurrence of fraud is highly uncertain. Different companies routinely rely on the expertise of professionals and the past fraud data to continually correct their databases, which in turn revives the situation.

2.1.3 Case Study: Supervised Learning in Insurance Fraud

A company old sly finds a fake claim by using logistic regression and random forests algorithms under supervised learning method. The model utilized features along with past claims history, the claim amount, and document discrepancies in training through historical claims data. As a result, the system was able to reduce the number of false payments by thirty percent and increase the fraud investigator output significantly within one year. Among the

2.2 Unsupervised Learning Approaches

Unsupervised learning, on the contrary of the supervised learning, does not demand for labeled data. Rather, it detects even the tiniest of lines of patterns and anomalies that might still refer to fraudulence. This is a way of finding the new frauds that were not announced thus far.

2.2.1 Clustering Techniques for Fraud Detection

Just like claims, clustering techniques, insurance companies can also use it to spot unusual trends.

- Claims are grouped together through K-Means clustering based on their similarities. Clusters with claims of the highest fraud risk may need to be referred to further investigation.
- Density-Based Spatial Clustering of Applications with Noise, or DBSCAN, is a method which is effective for finding isolated cases of fraud as it identifies those cases which are significantly different from all the other claims.

2.2.2 Anomaly Detection Methods

The high level of errors in claims is likely to be the issue that in essence makes fraud detection very much a business of anomaly discovery.

The usage of AI can identify discrepancies from fixed procedures of claim issuing:

- Using random segmenting of data, a machine learning method called isolation forests detects anomalies. Divergent from the usual, fraudulent claims are quickly separated**.**
- Deep learning auto encoders learn to reconstruct conventional assertions and find ones that significantly vary, therefore implying possible scam.

2.2.3 Use Case: Detecting Suspicious Claims with Anomaly Detection

A health insurance company seeing questionable claims utilizing anomaly detection. Examining elements including claim frequency, provider information, and treatment costs, the AI model found claims that varied from prior trends. This led to the

discovery of a dishonest system of clinics billing excessively.

2.3 Deep Learning and Neural Networks

Deep learning which involves the identification of intricate scam patterns of large scale dataset & hence leading to the development of scam prevention was carried out. Instead, techniques to isolate such connections on neural networks brought these opportunities for improvement.

2.3.1 How Neural Networks Improve Fraud Detection

Multiple layers within neural networks examine claim data to identify hidden fraud signals. Their particularly strong areas are:

- Learning complex fraud trends from several sources.
- Reducing false positives by separating real fraud from atypical but legitimate claims.
- Finding new fraudulent techniques by means of data adaption.

2.3.2 Applications of CNNs and RNNs in Fraud Detection

- Convolutional neural networks (CNNs) are used in most cases to manipulate images which are then used as proof of transactions, through which the identification of scams in the case of drastically changed invoices or wrongly made medical records, is done.
- Meanwhile, in the course of the claim's temporal diagnostic analysis, RNNs are ready to uncover the implicit manipulative practice including claimants who filed suspicious claims so often that the long period of time is enough to establish this.

2.3.3 Real-World Example of AI Implementation

One well-known motor insurer used deep learning to examine accident claim photos and spot differences. Convolutional neural networks (CNNs) helped to detect false claims including faked or exaggerated damage by means of a comparison of car damage images with historical accident data.

2.4 Hybrid Models and Ensemble Methods

Integration of several AI techniques improves scam detection accuracy. Using the benefits of several methods, hybrid models build a more strong detection system.

2.4.1 Benefits of Combining Multiple Models

- Improved prediction dependability by ensemble methods comes from the combination of several models.
- Improved scam detection covers supervised, unsupervised, & deep learning algorithms to find different scam trends.
- Integrated models help to distinguish real anomalies from fake claims, hence reducing false positives.

2.4.2 Stacking and Boosting in Fraud Detection

- Combining many models of logistic regression, decision trees, and neural networks allows one to create a meta-model improving fraud detection efficiency.
- Boosting-XGBoost, AdaBoost focusses on misclassified events and improves model precision over consecutive rounds. These approaches are quite successful in fraud detection.

2.4.3 Case Study: Hybrid Model in Insurance Fraud

Using supervised learning (random forests), unsupervised learning (auto encoders), & deep learning (convolutional neural networks), an insurer combined methods. Millions of dollars in reimbursements were saved when this system found bogus claims with 40% more accuracy than more traditional approaches.

3. Materials and Methods

Using AI-driven scam detection calls for a methodical approach including data collecting relevant information, choosing suitable ML models, & effective application of them. Data collecting, preprocessing, model selection, training, & implementation frameworks define the basic components of building an AI-driven scam detection system.

3.1 Data Collection and Preprocessing

Every AI-driven fraud detection system is built mostly on data. Excellent, painstakingly produced data helps machine learning systems to clearly separate real from fake claims.

3.1.1 Sources of Insurance Claim Data

- Finding insurance fraud requires the examination of large amounts of both structured and unstructured data from many sources.

Organized information includes numerical and category data kept in databases as well as:

- Economic claims.
- Data about the policyholder (age, residence, claims history).
- Documents related to financial transactions.
- Timestamps for claim submission.

Unstructured data is information with great insights however cannot be readily arranged into tables.

- Digital or handwritten claim records.
- Medical records and invoices.
- Emails, audio files, and call transcripts.
- Images and videos offered for claims.

Modern fraud detection systems improve accuracy by combining unstructured and ordered data.

3.1.2 Data Cleaning and Feature Selection

Raw data often shows anarchy with errors, missing values, and variances. Cleansing data improves model performance.

Data Cleaning:

- Removing repetitions & fixing incorrect entries
- Mean/mode imputation using statistical methods for missing data imputation.
- Standardizing forms (such as values for date and time, money units).

Feature Selection:

- Finding key elements that help to detect fraud
- Using techniques to remove superfluous elements include correlation analysis and decision trees.
- Appreciating domain knowledge to maintain important qualities A well-processed dataset reduces noise and enhances model efficiency.

3.1.3 Handling Imbalanced Datasets

Given real claims, instances of Scam are rather rare, which produces a distorted dataset. Trained on such data, ML techniques could find it challenging to correctly detect fraudulent claims.

Techniques to correct imbalance include:

- Oversampling: Increasing the number of scam cases by means of SMote (Synthetic Minority Over-sampling Technique) approaches.
- Reducing the number of valid examples will help to create a balanced dataset.
- Cost-sensitive Learning: Increasing fines for misclassification of false positives to improve fraud detection efficiency.

By balancing the dataset, the model becomes more adept in consistently spotting bogus claims.

3.2 Model Selection and Training

Good fraud detection depends on the suitable ML model used.

3.2.1 Selection Criteria for Machine Learning Models

Models of scam detection have to fulfill specific criteria:

- Improved Precision & Recall: The model has to minimize false positives & precisely identify misleading events.
- Capability to Identify Anomalies: Often erratic fraud calls for models that can change with new fraud patterns**.**

Scalability: The model has to effectively handle large databases.

Common approaches of machine learning for scam detection consist in:

- Effective for ordered data and easily interpretable, decision trees and random forests.
- Exceptions for organizing tabular data with outstanding performance are gradient boosting algorithms (XGBoost, LightGBM).
- Appropriate for complex patterns, especially in unstructured data (e.g., claim documents, images), are neural networks.
- Used in fraud detection systems to identify anomalies, auto encoders with isolation forests.

3.2.2 Training and Validation Process

Training a scam detection model requires labeled data deceptive claims against non-deceptive ones to help pattern recognition.

Key steps in training:

Splitting Data:

- Training set covering seventy to eighty percent of all the data
- Validation range (10–15 percent)
- Range of tests: 10–15%

Feature Engineering:

- Feature engineering is necessary for developing new features motivated by expert knowledge such as customer claim frequency.
- Using methods for coding categorical data.

Hyperparameter Tuning:

- Using grid search or bayesian optimization will help to improve model performance.

Cross-Validation:

- K-fold cross-valuation ensures the effectiveness of the model over several sets.

3.2.3 Performance Evaluation Metrics

To evaluate a scam detection system it is necessary that very specific criteria be met:

- **Precision**: It's the percentage of misleading events that are detected which are really misleading.
- **Recall**: Real scam cases are detected by the model in the exact count.

Evaluates whether the model distinguishes between non-misleading & misleading events.

ROC-AUC, or Receiver Operating Characteristic - Area under the Curve, is:

An efficient model achieves a strong equilibrium between these measures, hence reducing false positives and false negatives.

3.3 Implementation Frameworks

Once the model is selected, the coding and application procedures are put to use. [Callbacks] Overflow and the efficiency of the equipment or instruments employed will influence each other in a reasonably profound manner.

3.3.1 Overview of AI and Machine Learning Tools

Designers implement fraud detection systems by using many algorithms and libraries:

Scikit-learn:

- Old-fashioned AI models and languages, such as Random Forests and in case of Trees of decision, are noticed by Scikit-learn to be the most suitable tool.
- Offers thorough feature selecting powers and preprocessing tools.

TensorFlow & Keras:

Suitable for models of deep learning:

- Incorporating neural networks applied for text-based fraud detection or image-based one.
- advocates broad adoption grounded in GPU acceleration.

PyTorch:

Provides flexibility for building complex models including Graph Neural Networks (GNNs). Ideal for projects requiring research.

XGBoost & LightGBM:

- Rapid execution and great performance of XGBoost and LightGBM make them best for structured data.

- The suitable tool choice depends on the efficiency of the fraud detection model and the data features.

3.3.2 Cloud-Based vs. On-Premise Deployment

Once the model is completed, it has to be put into use in a manufacturing environment for actual time scam recognition. Companies have to choose from on-site or cloud-based deployment.

Cloud-Based Deployment (AWS, Google Cloud, Azure):

- Scalable, affordable & flawless API connection.
- Drawbacks include reliance on their internet access & some privacy concerns. On-Premise Deployment:
- Two benefits are improved by data security control & autonomous from their outside sources freedom.
- **Drawbacks:** Huge upfront setup costs and independent IT infrastructure is required.

Many insurers support a hybrid approach whereby sensitive information is kept on-site to satisfy legal requirements & the cloud is used for maximum scalability.

4. Results and Discussion

4.1 Performance of Different Models

Artificial intelligence and machine learning have greatly improved insurance industry fraud detection. Different machine learning techniques are used to detect false behavior; each has advantages and disadvantages. Factors like practical application, feature selection, and data quality define the effectiveness of these models.

4.1.1 Comparing Various Machine Learning Models

Usually employed as the benchmark, logistic regression is a simple and understandable model. It struggles with complex fraud patterns even if it runs efficiently on structured data. The coding and application procedures start when the model is chosen. If not more, the convergence of the holes about the plans and the operational tools employed will provide good feedback to a major degree. By giving weights to mistakes from past iterations, Gradient Boosting Machines (GBM) models XGBoost and LightGBM improve decision trees and hence increase their effective fraud detection capacity.

Deep learning neural network models search large databases in order to find complex trends. Highly exact, they need large datasets and are frequently seen as black-box models, therefore impeding interpretability. Unsupervised models like Autoencoders and Isolation Forests are particularly suited for spotting, developing and changing fraudulent tendencies as they run independently of labeled fraud events.

4.1.2 Benefits and drawbacks of many methods

Every model has advantages and drawbacks:

- Although logistic regression & the decision trees are interpretable, conventional ML models may lack the complexity needed to detect their complicated fraud schemes.
- Although they need significant processing resources, ensemble techniques (Random Forest, Gradient Boosting) improve accuracy via the combination of their several models.
- Deep learning models need significant training data and show a lack of transparency even if they are rather efficient for processing big amounts of information.

This approach is good for revealing hitherto undetectable fraud patterns; yet, it may sometimes produce false positives, which would lead to unnecessary investigations.

4.2 Case Studies and Useful Notes

Global insurance companies are tackling fraud using AI, varying in degree of success. Some empirical cases showing the effectiveness of their AI-enhanced fraud detection are shown here.

4.2.1 AI Applied in Notable Insurance Companies

Many of the big companies, like Allstate, Geico & AXA, have implemented AI-driven fraud detection into their claims handling systems. These companies examine claims data using ML techniques to find dubious activities worthy of their further investigation. While reducing fraudulent disbursements, AI has enabled insurers' accelerated processing of claims.

4.3 Difficulties and Moral Considerations

Although AI brings challenges, particularly with regard to bias, privacy & regulatory conformity, its application in their fraud detection has great advantages. These ethical concerns have to be carefully addressed to ensure that AI-driven fraud detection maintains fair, open & legally compliant character.

4.3.1 AI Preference Models and Approaches for Reducing

AI models are mostly reliant on the information; so, if the training data is biased, the model could reinforce & worsen such prejudices. Skewed data in fraud detection might lead to their overactive investigation of certain consumer groups, areas or demographics, therefore producing faulty fraud charges.

Common forms of bias in AI fraud detection consist of:

- Historical Bias: Should previous fraud investigations have disproportionately found certain groups, AI might learn to target such groups once again unfairly.
- Sampling bias: A lack of variation in the training data might make the model less able to generalize, hence producing faulty fraud classifications.
- Algorithmic bias: Some ML techniques may naturally give some data points top priority, hence producing their misleading results.

Insurance companies might employ the following techniques to reduce these biases:

- Diverse and Representative Data: Ensuring that training sets include a range of circumstances to prevent the overrepresentation of certain groups helps to prevent this overrepresentation of some groups.
- Fairness testing and bias audits methodically evaluate models for bias and change training data as needed.
- Human Oversight: Using artificial intelligence as a tool for decision-support rather than a totally automated fraud detection system will allow human investigators to confirm claimed events.

Explainable artificial intelligence (XAI) is the deployment of AI models with open explanations for fraud predictions to help to detect and correct biases.

4.3.2 Regulatory Adherence and Privacy Issues

Extensive client information is required for their AI fraud detection, which causes privacy, data security & the conformity to international regulations like concerns about:

- The General Data Protection Regulation (GDPR) guarantees customers their right to be informed about the use of their information & the requirements that companies maintain transparency in the AI decision-making.
- Granting consumers control over their privacy information, the California Consumer Privacy Act (CCPA) imposes strict responsibilities on businesses handling their consumer information.
- Policies Regarding Insurance Many national regulations control the use of AI in insurance fraud detection, so equality, transparency & respect of anti-discrimination laws become even more important.
- Implement strong data encryption to protect their private customer information from breaches & their illegal access thereby addressing their privacy issues & preserving their compliance.
- Use Privacy-Conserving AI Methodologies: Differential privacy & federated learning let AI learn from data while protecting their personal information.
- Providing customers with clear data use instructions & making sure AI-generated decisions are understandable & open for dispute will help to guarantee transparency & explainability.

Reducing bias & addressing privacy concerns would help AI-driven fraud detection to be both effective & socially conscious, hence retaining public trust and helping to fight fraud.

4.4 Future Directions

Artificial intelligence is accelerating and its use in fraud detection will always keep developing. Future developments will focus on improving the accuracy, flexibility, and openness of fraud detection.

4.4.1 New AI Tools for Detection of Fraud

Many newly developed artificial intelligence systems are ready to improve fraud detection powers:

- Graph neural networks (GNNs) look at the relationships among entities e.g., policyholders, claims, service providers to find coordinated fraud networks.

- By letting AI learn from unprocessed information, self-supervised learning lowers the need for huge scale labeled datasets & improves the discovery of latest fraud trends.
- By allowing insurers to collaborate on the fraud detection without sharing raw information, FL helps to safeguard privacy & increase their effectiveness of fraud detection.
- Artificial intelligence systems are being developed to find synthetic identities used in false claims, deepfake images, and videos used in frauds.

These technologies will improve fraud detection accuracy and allow insurance companies to surpass more sophisticated fraud schemes in speed.

4.4.2 Explainable AI's role in Improving Fraud Detection Transparency

The "black box" feature of many models hampers the understanding of decision-making procedures and is a major issue in artificial intelligence-driven fraud detection. Through improved interpretability and responsibility of AI models, explainable artificial intelligence (XAI) aims to solve this problem.

Explainable artificial intelligence offers mostly two main benefits for fraud detection:

- Improved Transparency and Trust: Consumers and authorities will be able to understand the justification for a claim labeled as untrue.
- Fair Decision-Making – Helps insurance companies find and fix flaws in their fraud detection systems.
- Guarantees of AI-driven fraud detection that follow legal requirements demanding openness in automated decision-making constitute regulatory compliance.

AI transparency is improved by use of methods such LIME (Local Interpretable Model-agnostic Explanations) and SHAP (Shapley Additive Explanations). Using explainable AI will help insurance companies create fair and strong fraud detection systems. The balance of openness, privacy, and accuracy will determine artificial intelligence's course in fraud detection. Insurance companies have to use ethical artificial intelligence techniques to ensure fairness as technology develops and to be aggressive against fraudsters.

5. Conclusion

With billions in losses annually & impacting both insurance companies & actual policyholders, insurance fraud is a major issue. While somewhat effective, conventional fraud detection methods struggle to fit the growing complexity of fraudulent tactics. Providing quick, accurate & flexible answers, AI and ML have become powerful weapons in the battle against dishonest activities. By analyzing vast information, finding hidden patterns & always learning from the latest fraud schemes, AI-driven systems may identify bogus claims more successfully than their rule-based methods.

AI's ability to extensively examine the both structured & unstructured data both significantly helps with their fraud detection. Like decision trees, neural networks & their anomaly detection algorithms, ML methods might expose alarming trends that human researchers would ignore. These solutions let insurance companies spot fraudulent claims in actual time, therefore reducing their financial losses & improving their operational effectiveness. Furthermore, latest AI approaches such as FL & graph neural networks help to find their fraud networks while maintaining their data security.

Using AI to identify fraud creates a lot of challenges. In AI models, bias might lead to unfair targeting of certain groups; privacy concerns over consumer information call for careful monitoring. GDPR and CCPA highlight the requirement of transparency and force insurance companies to provide justice and clarity in AI-driven decisions. Explainable artificial intelligence (XAI) is becoming more and more important in reducing these problems as it helps stakeholders to understand the reasoning behind the decisions of fraud detection systems.

For the insurance industry, the consequences of AI-driven fraud detection are major. Reducing faulty disbursements can help insurers reduce their prices, therefore enabling more fair rates for their customers. Improved risk assessments made possible by AI help insurance companies to maximize their policies & their claim processing. Insurers have to keep investing in their AI technology as dishonest tactics develop, improving their models via constant learning, regulatory adherence & the elimination of their bias.

Improving accuracy & openness will become more important in the AI fraud detection going forward. Though AI-driven fraud detection has proven great effectiveness, further developments in the explainability, privacy-preserving techniques & the

ethical AI methods will be more crucial. Equilibrium between automation & the human oversight allows insurance companies to create fair & strong fraud detection mechanisms. In a time of increasingly educated fraudsters, AI offers a vital & flexible defense that, with careful usage, may greatly improve the insurance industry.

References

[1] Joginipalli, S. K., & Gummadi, V. (2024). *Advancing Insurance Fraud Detection: Leveraging Machine Learning and AI Techniques.*

[2] Sharma, R., Mehta, K., & Sharma, P. (2024). Role of Artificial Intelligence and Machine Learning in Fraud Detection and Prevention. In *Risks and Challenges of AI-Driven Finance: Bias, Ethics, and Security* (pp. 90-120). IGI Global.

[3] Srinivasagopalan, L. N. (2022). AI-enhanced fraud detection in healthcare insurance: A novel approach to combatting financial losses through advanced machine learning models. *European Journal of Advances in Engineering and Technology*, *9*(8), 82-91.

[4] Gangani, C. M. (2024). AI in Insurance: Enhancing Fraud Detection and Risk Assessment. *International IT Journal of Research, ISSN: 3007-6706*, *2*(4), 226-236.

[5] Ejiofor, O. E. (2023). A comprehensive framework for strengthening USA financial cybersecurity: integrating machine learning and AI in fraud detection systems. *European Journal of Computer Science and Information Technology*, *11*(6), 62-83.

[6] Agarwal, S. (2023). An intelligent machine learning approach for fraud detection in medical claim insurance: A comprehensive study. *Scholars Journal of Engineering and Technology*, *11*(9), 191-200.

[7] Narne, H. (2024). Machine Learning for Health Insurance Fraud Detection: Techniques, Insights, and Implementation Strategies.

[8] Saddi, V. R., Gnanapa, B., Boddu, S., & Logeshwaran, J. (2023, December). Fighting Insurance Fraud with Hybrid AI/ML Models: Discuss the Potential for Combining Approaches for Improved Insurance Fraud Detection. In *2023 4th International Conference on Communication, Computing and Industry 6.0 (C216)* (pp. 01-06). IEEE.

[9] Pareek, C. S. From Detection to Prevention: The Evolution of Fraud Testing Frameworks in Insurance Through AI. *J Artif Intell Mach Learn & Data Sci 2023*, *1*(2), 1805-1812.

[10] Reddy, S. R. B., Kanagala, P., Ravichandran, P., Pulimamidi, R., Sivarambabu, P. V., & Polireddi, N. S.A. (2024). Effective fraud detection in e-commerce: Leveraging machine learning and big data analytics.

[11] *Measurement: Sensors*, *33*, 101138. Pala, S. K. (2022). Investigating fraud detection in insurance claims using data science. *International Journal of Enhanced Research in Science, Technology & Engineering ISSN*, 2319-7463.

[12] Dwadasi, A. (2024). Artificial intelligence and machine learning in financial services: risk management and fraud detection. *J. Electrical Systems*, *20*(6s), 1418-1424.

[13] Bansal, U., Bharatwal, S., Bagiyam, D. S., & Kismawadi, E. R. (2024). Fraud detection in the era of AI: Harnessing technology for a safer digital economy. In *AI-Driven Decentralized Finance and the Future of Finance* (pp. 139-160). IGI Global.

[14] Lai, G. (2023). Artificial Intelligence Techniques for Fraud Detection. *Preprints*, 2023121115.

[15] S. S. Nair, G. Lakshmikanthan, N. Belagalla, S. Belagalla, S. K. Ahmad and S. A. Farooqi, ""Leveraging AI and Machine Learning for Enhanced Fraud Detection in Digital Banking System: A Comparative Study,"" 2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT), Bhimtal, Nainital, India, 2025, pp. 1278-1282, doi: 10.1109/CE2CT64011.2025.10939756.

[16] Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., ... & Saif, A. (2022). Financial fraud detection based on machine learning: a systematic literature review. *Applied Sciences*, *12*(19), 9637.