

A Comprehensive Survey of Recent Advances Artificial Intelligence for Insurance Fraud Detection

Dr. Amit Jain¹

¹ Professor, Department of Computer Science and Engineering, OP Jindal University, Raigarh(C.G), India

ABSTRACT: Insurance fraud is a big problem that the insurance industry is trying to solve. Economic loss, operational costs, and a decline in consumer trust are all consequences of insurance fraud. Traditional techniques of fraud detection, such as rule-based systems and human processes, frequently fail to detect more sophisticated fraud schemes. By analyzing complicated data in real-time, artificial intelligence (AI) has been shown to be an effective tool for automating the identification of fraud. Machine learning, explainable AI, federated learning, deep learning, reinforcement learning, natural language processing, and the most current approaches to AI methods in insurance fraud detection are included in this review. The paper also contains a discussion on traditional fraud detection methods, most popular insurance frauds, data preprocessing methods and some common metrics. Additionally, it looks at the latest research studies and points out the advantages and disadvantages of the available AI-driven approaches. Data quality, class imbalance, privacy preservation, model interpretability, scalability and regulatory compliance are among the key challenges that are critically analyzed.

KEYWORDS: Insurance Fraud Detection, Artificial Intelligence (AI), Machine Learning, Deep Learning, Fraud Analytics, Explainable Artificial Intelligence (XAI), Introduction.

1. Introduction

In today's culture, insurance plays a significant role. The insured party pays a premium to an insurer, and the insurer promises to pay a specified amount in the event that the insured party suffers a loss of an insurable interest as a result of one or more future, clearly stated, but unknown occurrences. This protects the insured party from the danger of incurring unmanageable financial harm [1]. Insurance fraud represents a growing concern for the global insurance industry, contributing to billions of dollars in annual losses. Fraudulent activity is not only bad for insurance companies' financial health, but it also increases costs for policyholders, which means it has a negative effect on both consumers and insurance companies [2]. Significant financial losses and an increase in the requirement for efficient fraud detection systems have resulted from insurance fraud, which has recently emerged as a major problem for the insurance sector [3]. There is an imbalance in the data related to insurance fraud detection and fraud detection in general. A high success rate for valid case predictions is achieved using the data in its current state, while no fraudulent instances are predicted. By entering into an insurance policy, a person or organization can secure financial

protection or payment from an insurance provider in the event of a loss [4]. The insured can save money on premiums since the business combines their risks. There are three main reasons why customers choose insurance policies nowadays. (i) investment; (ii) tax; and (iii) risk element. Nowadays, people's lives are filled with unforeseen challenges, such as accidents and health issues. A person can suffer tremendous loss in the event of an accident [5]. Therefore, everyone wants to be able to preserve their own life, and everyone needs a plan B. People who have been in accidents and are now ill can get assistance from their insurance company [6][7][8]. Currently, customers are inputting all the details using paper forms. After that, it was scanned and saved as a PDF [9]. Then the internal auditor manually entered the data into the database. False statements were made because the internal auditor was incompetent or careless. The insurance industry and its customers may suffer unforeseen losses as a result of these factors. Relinquish all legal papers when enrolling in an insurance program and furnish the proper paperwork to get payment from the program. This is not occurring while the insurance coverage is being processed.

The fraud detection sector stands to be profoundly affected by the application of AI [10]. ML and DL are

being used more and more by AI-based systems to find suspicious trends in big datasets, spot fraudulent activity as it happens, and cut down on financial losses. These systems have proven effective in various industries, such as banking, insurance, and healthcare, and are being widely studied and discussed for their potential to enhance financial fraud prevention processes [11]. AI-powered systems can, for example, ingest and analyze a tremendous amount of data at a much faster rate than traditional systems, which would make fraud detection quicker and more accurate in comparison to the traditional way of doing it [12][13]. These AI systems can adapt and become more effective at identifying fraud over time, as they learn from previous instances of fraud [14][15]. There are some positive aspects of AI, but there are also some negative aspects of using AI to identify fraud. There have been discussions on the ethical implications of using AI in healthcare and financial services, where there is a high potential for privacy violations, algorithmic biases, and data breaches [16].

A. Structure of Paper

The paper is organized as follows: Section II presents the issue of insurance fraud and traditional approaches to detecting insurance fraud. Section III reviews AI techniques for insurance fraud detection. Section IV discusses recent research and comparative analysis. Section V highlights key challenges and limitations, while Section VI concludes the paper and presents future research directions.

2. Insurance Fraud Detection: Concepts and Foundations

The goal of any action taken with the knowledge that it could lead to an inaccurate insurance claim is to commit insurance fraud [17]. This may occur if the insurer wrongfully withholds a benefit or if the claimant attempts to get a benefit that is not lawfully theirs. Both policyholders and personnel of insurance companies are susceptible to falling victim to these scams. Filing an insurance claim with the purpose of misleading an insurer is known as a false insurance claim. Insurance fraud has been present in some form or another since the industry's inception. Claims that are not legitimate, or fraudulent, cost insurers billions of dollars annually [18].

A. Types of Insurance Fraud

Insurance fraud encompasses a wide variety of unethical practices committed in pursuit of illegal financial benefits and can occur in a variety of insurance sectors. The major types of insurance fraud are classified based on the insurance domain and the nature of the fraudulent activity.

1) Health Insurance Fraud

The most common types of healthcare insurance fraud are either fraudulently charging another party for services rendered or using one's benefits to cover prescription drugs prescribed by someone other than one's own doctor. A health insurance company is tricked into paying out fraudulent benefits to the policyholder, another customer, or the service provider in this sort of fraud by being supplied false or misleading information. Health care providers or the individual themselves can carry out these kinds of tasks [19].

2) Automobile Insurance Fraud

This type of fraud occurs when individuals deliberately provide false or misleading information to obtain financial benefits from vehicle insurance claims[20]. Such deceptive practices may involve fabricating evidence, misrepresenting the circumstances of an accident, or submitting claims for losses that did not occur as reported. Common examples include staged accidents, fraudulent injury claims, false reports of vehicle theft, claims for accidents alleged to have occurred after policy activation, claims for pre-existing vehicle damage, and concealing the identity of an uninsured driver involved in an accident. Due to the high costs and decreased reliability caused by these fraudulent actions, insurance carriers suffer significant financial losses [21].

3) Motor Insurance

Fraud involving personal damage claims that occurs both before and after insurance is included in this category. Typically, vehicle, accident, claimant, driver, injury, treatment, lost income, and other categories are used to categorize binary indications in automobile insurance data. The only publicly accessible dataset for fraud detection research is a small one for vehicle insurance. Legal and competitive considerations make it very difficult to obtain actual company data for research objectives. One possible solution to the data availability issues is to generate synthetic data that closely resembles real data in order to target certain types of fraud. In most cases, there are two main forms of car insurance fraud:

- **Hard frauds:** This is purposefully wrecking the vehicle in order to get rid of it quickly or get more money out of it than what it would be worth on the market. For instance, it may be stolen, set on fire, crashed into a river, or lost due to an unanticipated event. A genuine accident might happen, but the unscrupulous owner could use the chance to add up all the little damage to the car from the past and charge it to the actual accident.
- **Soft fraud:** This is the main reason why most car insurance scams occur. Many claims for a single loss, exorbitant repair costs, damage done at an earlier date,

needing to replace outdated spare parts, etc [22].

- **Policy Fraud:** Providing false information to obtain lower premiums.
- **Claims Fraud:** Exaggerating damages, submitting fake medical bills, or staging accidents.
- **Identity Fraud:** Using stolen or synthetic identities to file fraudulent claims.
- **Provider Fraud:** Involves healthcare or auto repair professionals inflating costs or billing for services not rendered[23].

3. Recent Ai Techniques for Insurance Fraud Detection

The ability of systems that identify insurance fraud has been substantially improved by new developments in artificial intelligence. In order to better detect hidden patterns of fraud and adapt to new fraud tactics, AI systems can scan complicated information and massive volumes of data. The techniques help in making better decisions, reducing false positives and identifying suspicious insurance claims early.

A. Evolution of AI in Fraud Detection

In the last decade, AI has made significant strides in fraud detection. The existing systems were rule-based and flagged any deviation from a set of rules, but they had the following drawbacks: They failed to adapt to new forms of fraud, and they were based on static rules. AI systems have become more dynamic and now feature ML enabling them to learn from previous data and warn of anomalies that may pass undetected by humans. Insurance firms are now able to stay ahead of insurance fraudsters, who are always discovering new ways to elude detection, thanks to this shift [24]. AI systems can process immense data, making them adept at spotting intricate fraud strategies that span many transactions and involve numerous players.

B. AI-Based Approaches for Insurance Fraud Detection

The insurance domain is an area with high-dimensional class imbalance and adversarial behavior, which makes fraud detection difficult. Insurers have historically detected questionable claims using rule-based expert systems and human checks [25]. Another problem with these systems is that fraudsters may easily exploit them because of how well they adapt to new fraud schemes [26].

C. Machine Learning Models for Insurance Fraud Detection

ML is an integral part of AI-powered fraud prevention systems. One such technique is supervised

learning, in which a set of claims, called a labeled dataset, is provided with labels marking them as true or false. These are used to train the fraud detection models to recognize patterns associated with fraudulent transactions. The goal is to use supervised learning algorithms like DTs, SVMs, and NNs to learn complicated relationships in the data, and then use these associations to classify new claims.

- One of the most common methods for detecting fraudulent claims is supervised learning, which involves training models using labeled data. Using historical data, these models can determine the probability of fraud.

- There is no need for labeled data in unsupervised learning. Rather, it uses claims data to uncover new forms of fraud that were previously unknown. In this context, clustering and autoencoders are common algorithms employed. Outlier detection or unusual pattern detection can be employed via clustering algorithms for fraud detection. An Autoencoder, a form of NN, is used to rebuild the input data, and statements that are very different from the rebuilt one are flagged as probable fraud. When determining a new fraud pattern, supervised learning can be very useful if there are patterns that are not observed or labeled during training.

D. Natural Language Processing (NLP)

Insurance claim text data is a major application of NLP for analysis [27]. The language in claim descriptions, customer interactions, and communication logs can all be analyzed using NLP to detect inconsistencies or deceptive language, which may indicate fraudulent behavior. Furthermore, NLP can be used to identify suspicious activities or relationships within the unstructured data of social media sources that might indicate fraud. The capability of real-time analysis of massive amounts of text information can help reveal the veracity of claims and improve the fight against fraud.

E. Data Analytics and Predictive Modeling

Data analytics and predictive modeling are vital to comprehending trends and patterns in fraudulent claims, as well as predicting potential future fraudulent claims. The data can be analyzed for trends in claims that might indicate fraud such as unusual payouts, changes to claimant information and a rise in claim numbers from a specific area etc. Historical trends are then used to make predictions of fraud in a claim with predictive modeling techniques such as logistic regression and ensemble models. These models can be updated frequently with new data and can identify new fraud patterns and thus predict fraud in real time, enabling insurers to prevent losses ahead of time [28].

F. Reinforcement Learning for Insurance Fraud Detection

RL models are adaptive, meaning they adaptively adjust the threshold for fraud detection in their relationship with their surrounding environment. The models are optimized over time between accuracy and false positives. For example, insurance companies could use reinforcement learning to review high-risk claims and automatically get low-risk claims [29].

G. Federated Learning for Insurance Fraud Detection

Federated learning has emerged as a significant facilitator for collaborative fraud detection without centralized data sharing [30]. This is in response to the increasing number of rules and issues about data privacy. Graph Attention Networks (GAT) and differential privacy (DP) in conjunction with FL have produced quite accurate outcomes, as seen in FinGraphFL. Similarly, efficacy and transparency are enhanced when federated learning and blockchain are combined. CCFD is suitable for more powerful applications compared to other fragmented data applications that are not as costly to implement centralized data collection, including e-learning platforms for numerous campuses [31] or groups of autonomous robots in distinct environments [32].

H. Deep Learning Techniques for Insurance Fraud Detection

DL is one of the subfields of AI that works with massive amounts of data through neural networks. These models have a distinctive ability to detect patterns, which makes them useful for detecting fraudulent claims and increasing underwriting accuracy. Decomposing the DL process into computational layers enables the model to discover hidden patterns in data, extract patterns from historical data, and forecast patterns in future data.

1) Feedforward Neural Networks (FNNs):

The network type is frequently used to identify fraudulent claims from a set of inputs such as claim value, claim experiences of the policyholder, and reported events. The network can also use previous information to make a decision, and when it sees inconsistencies or patterns that might be indicators of fraud.

2) Convolutional Neural Networks (CNNs)

CNNs were originally designed to recognize images and are used for insurance fraud detection to process visual information, such as photos of accidents or scanned documents submitted as part of an insurance claim. Such networks can identify any discrepancies or adjustments between pictures and the extent of damage, and can identify cases of fraud during the claims process.

3) Recurrent Neural Networks (RNNs):

RNNs work well with sequential data. They are able to evaluate the order in which claims have been submitted by a specific individual and identify if there are any trends in fraud over time, which can be helpful when investigating insurance fraud. RNNs can also be used to monitor the behavior changes of a claimant, and identify persistent trends that could indicate fraud.

4. Impact of Ai On Insurance Companies

AI can transform the insurance industry in various domains, such as client underwriting, claims processing, marketing, and detecting fraud. Claim settlement relies on semi-structured or unstructured data in an iterative way, such as data from medical reports, incident documentation, and repair estimates, as well as claim forms. Evaluation and decision-making about claim authenticity and fraud prevention are aided by the data [33]. By streamlining the process, insurers may save time by automatically accessing and extracting key information from claims. It aids insurers in expediting claims processing while cutting costs and improving customer experience using clever automation or RPA (robotic process automation). Data patterns allow for the easy detection of fraudulent claims. Automation of damage evaluation, prediction of expenses from previous data, and learning and discovery of novel case scenarios are all made possible by ML. Innovative services for target personas are the goal of AI. The goal is to leverage technology to boost production, automate processes, and introduce new services that improve customer interaction, which in turn might bring in new consumers and make existing ones happier, more loyal, and more invested in the brand.

Reduced costs, improved customer experience, fraud detection, claims automation, underwriting, and new product and service development are all outcomes of AI.

- Assists in making wiser, quicker, and more precise choices.
- Helps identify regions or patterns that a person would miss.
- Offers enhanced risk coverage and analysis of both current and future threats.
- Enhances the capacity to assess risk [34].

A. Challenges and Limitations of AI in Insurance Fraud Detection

AI provides significant benefits in the field of insurance fraud detection, there are several notable challenges that come with it. It is essential for insurers to be aware of these limitations to ensure they can use AI in an ethical, compliant, and sustainable manner.

1) Data Quality and Availability

A high-quality, comprehensive, and accurately represented dataset is essential for training AI models, and these factors determine the models' efficacy. Bias and inaccuracies in insurance data from past transactions and missing information in the databases may lead to inaccuracies in the fraud detection systems. Policy pricing and claims approval disparities might persist if data is inaccurate or incomplete [35]. Furthermore, the lack of data across sectors can limit the potential of AI's prediction, particularly in new insurance business segments.

2) Model Transparency and Explainability

This "black box" process behind many of the models utilized by complex AI is similar to deep neural networks, and insurers, regulators, and customers cannot fully understand how the decision is made. The ambiguity can lead to mistrust and accountability issues, especially when claims are denied or premiums are adjusted, depending on AI outputs. XAI frameworks are being developed that are clear; however, there are challenges because of the performance impact.

3) Regulatory and Legal Constraints

The insurance sector is a very regulated sector. Australian law and overseas law offer protection for AI systems to ensure data is covered, and to prevent discrimination and financial abuse. AI decisions could be subject to regulation, making operations more complex and potentially complicating matters. Documentation and traceability of AI decisions might be regulated, making operations more complex and potentially complicating matters. Regulatory requirements also contribute to both the operational and legal complexity of documentation and traceability of AI decisions. The corporation risks financial penalties, reputational harm, and other negative outcomes if it does not adhere to regulatory standards.

4) Ethical and Privacy Concerns

AI-driven fraud prevention tools can be complex and require extensive personal and behavioral data. The ethical issues involve privacy, consent and misuse when collecting, processing and analyzing such data. Insurers need to be clear on their ethical guidelines and policies to prevent AI from discriminating against vulnerable groups without their intent [36].

5) Overfitting and False Positives

Modeling with overly large amounts of historical data can lead to overfitting, where the model is optimized for past cases but struggles to perform well in new, unseen scenarios. This can create wrong claims

and therefore cause inefficiencies in the operation and harm to the customer relationship.

6) Integration with Legacy Systems

AI-powered platforms may not be compatible with many insurance businesses' current IT systems. Small or resource-limited insurers may find the upfront expense of implementing sophisticated AI solutions, such as the purchase of software and hardware and staff training, too high [37].

5. Literature Review

This section includes a summary of previous research on a similar topic and some keywords relevant to the research. Table I compares recent insurance fraud detection research using AI techniques and identifies the methodologies used, their findings, benefits, risks, and recommendations for further research to make fraud detection more accurate and secure.

Priya (2026) introduces the ClaimGuardAI framework, a smart decision-support tool that uses structured data analytics and ML to identify insurance claims that are false. The framework includes features that help with data preparation, dealing with class imbalance, and comparing different classification algorithms. Scalable insurance claim processing is supported, automated fraud detection is enabled, suspicious claims are prioritized, detection accuracy is improved, and manual investigation efforts are reduced [38].

Peykani and Kugu (2026) The suggested architecture makes use of supervised ML models including XGBoost, DT, AdaBoost, Gradient Boosting, SVM, KNN, NB, and RF. SHAP is interpretable since it describes feature contributions. SHAP's interpretability stems from the fact that it details the contributions of features. Experiments showed that XGBoost surpassed the competitors with an F1-score and accuracy of 98.02%, proving that qualities related to defects and rules are crucial for fraud detection [39].

Agarwal et al., (2025) using a labeled dataset consisting of over 10,000 insurance policies, employ and assess eleven ML models to identify instances of insurance fraud. Performance is evaluated using the F1-score, recall, accuracy, and precision. With improved accuracy of fraud detection, generalizability, and reduced financial losses for insurance firms, ensemble models—particularly RF and Gradient Boosting models—produced the greatest results [40].

Gupta et al., (2024) ML approaches for insurance fraud detection using real-world insurance data. Compares different models like SVM, DT, RF, AdaBoost, Gradient Boosting, Stochastic Gradient Boosting, Extra Trees. The top models for improving insurance fraud

detection strategies are found by comparison analysis using accuracy, precision, recall, F1-score, and confusion matrices [41].

Rijanto et al., (2023) offer a solution to the issue of class imbalance by outlining a process for identifying insurance fraud utilizing the SMOTE and ADASYN methodologies. An ensemble of voters performs 10 rounds of cross-validation on SVM, RF, Balanced RF, and XGBoost before calling it a day. According to the findings, the SVM-SMOTE had the highest

performance, with an F1 score of 98% [42].

Sethi, Sing and Sarangi (2022) suggest an approach to healthcare insurance fraud detection that combines blockchain and DL. Secure, immutable, and traceable medical record management is ensured by blockchain, and DL can identify fraudulent claims. Experimental tests on real hospital datasets have shown that the fraud detection is more accurate, the data is more secure, and the medical insurance claim evaluation is more efficient [43].

TABLE I. COMPARATIVE ANALYSIS OF RECENT STUDY ON INSURANCE FRAUD DETECTION

Reference	Approach	Findings	Advantages	Challenges	Recommendations
Priya (2026)	Proposed ClaimGuardAI using machine learning with preprocessing, feature encoding, normalization, and class balancing for insurance fraud detection.	Achieved effective fraud classification with balanced accuracy, precision, recall, and F1-score while reducing financial losses.	Automated fraud risk assessment, reduced manual investigation, scalable deployment, improved detection accuracy.	Performance depends on quality of historical labeled datasets and proper data preprocessing.	Integrate advanced ML models and continuously update datasets to improve fraud detection performance.
Peykani and Kugu (2026)	Compared nine supervised ML models (RF, XGBoost, SVM, KNN, DT, AdaBoost, etc.) with SHAP and LIME explainability.	XGBoost achieved 98.02% accuracy and 98.02% F1-score. XAI identified important fraud-related features.	High prediction accuracy with explainable AI support for decision-making.	Class imbalance and need for model interpretability.	Employ XAI techniques such as SHAP and LIME with ensemble models for transparent fraud detection.
Agarwal et al. (2025)	Evaluated 11 ML models including ensemble methods using a labeled insurance dataset.	Random Forest and Gradient Boosting provided superior accuracy and generalization.	Improved fraud detection accuracy and reduced financial losses.	Model performance depends on dataset quality and balanced training data.	Adopt ensemble learning methods for large-scale insurance fraud detection.
Gupta et al. (2024)	Compared SVM, Decision Tree, Random Forest, AdaBoost, Gradient Boosting, SGD, and Extra Trees.	Comparative analysis showed ensemble methods outperform individual classifiers.	Comprehensive evaluation using accuracy, precision, recall, F1-score, and confusion matrix.	Selecting the optimal ML algorithm for different datasets.	Use comparative model evaluation before deployment in insurance systems.
Rijanto et al. (2023)	Applied SMOTE and ADASYN with SVM, RF, BRF, and XGBoost using ensemble voting.	SVM with SMOTE achieved F1-score >98%.	Effectively handled class imbalance and improved prediction performance.	Highly imbalanced fraud datasets.	Apply oversampling techniques such as SMOTE or ADASYN before model training.
Singh and Sarangi (2022)	Proposed blockchain and deep learning-based healthcare insurance fraud detection framework.	Improved fraud identification while ensuring secure medical record management.	Enhanced security, immutability, and traceability of healthcare records.	Complexity of blockchain integration and computational overhead.	Integrate blockchain with AI for secure and trustworthy healthcare insurance fraud detection.

Research Gap: There are still a number of issues that need fixing with insurance fraud detection systems that use AI. The majority of the studies around the concept are based on small and unbalanced datasets, which limits generalizability of their model to other insurance fields. Moreover, challenges for implementation include data privacy, model interpretability, scalability, and legal issues. Also, current approaches cannot detect new fraud patterns or penetrate the concept drift in real-time

as it happens. Future research should focus on building explainable, privacy-preserving, scalable, and adaptable AI frameworks that boost detection accuracy and assure transparency, robustness, and efficacy across multiple insurance situations.

6. Conclusion And Future Work

AI has transformed the insurance fraud detection system, making it more efficient, speedy, and automated.

Traditional fraud detection techniques and some new techniques like AI, particularly ML, DL, RL, federated learning, explainable AI and NLP were included in the survey. The studies examined here demonstrate the potential for AI-driven models to more accurately detect intricately woven fraud patterns, increase operational efficiency, and reduce losses. However, there are several challenges to be addressed, including the quality of the data, data imbalance, privacy and confidentiality, lack of interpretability of models, scaling, and regulatory compliance. These obstacles must be overcome if insurance companies are to successfully use fraud detection systems driven by AI.

This is a point of interest that will be continued in the future in the field of explainable, privacy-safe, and resilient AI models to adapt to new threats in fraud detection and prevention. Fraud detection and client data security might be enhanced with the use of LLM models in conjunction with federated learning, graph-based learning, and multimodal data analysis. Moreover, benchmark datasets and real-time assessment frameworks will help develop scalable, transparent, and trusted AI solutions for the next generation of insurance fraud detection.

REFERENCES

1. G. Schrijver, D. K. Sarmah, and M. El-hajj, "Automobile insurance fraud detection using data mining: A systematic literature review," 2024. doi: 10.1016/j.iswa.2024.200340.
2. S. Kakkar, B. Makkena, A. Chaudhary, and A. Kakkar, "Explainable Machine Learning Models for Credit Scoring for Risk Forecasting in Big Financial Datasets," in 2026 2nd International Conference on Cognitive Computing in Engineering, Communications, Sciences and Biomedical Health Informatics (IC3ECSBHI), Greater Noida, (Delhi NCR), India: IEEE, 2026, pp. 1384–1391, February. doi: 10.1109/IC3ECSBHI67834.2026.11469004.
3. S. R. Somula, "Intelligent Fraud Prevention: Implementing AML Solutions For Mcca Reimbursement Claims Protection," *Int. J. Comput. Eng. Technol.*, vol. 16, no. 1, pp. 3609–3622, Feb. 2025, doi: 10.34218/IJCET_16_01_249.
4. C. Phua, D. Alahakoon, and V. Lee, "Minority report in fraud detection," *ACM SIGKDD Explor. Newsl.*, vol. 6, no. 1, pp. 50–59, Jun. 2004, doi: 10.1145/1007730.1007738.
5. H. K. Yadav, "Design and Implement Machine Learning Based Predictive Analytics for Road Safety and Accident Prevention," in 2026 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), IEEE, Mar. 2026, pp. 1–6. doi: 10.1109/IATMSI68868.2026.11465965.
6. A. K. I. Hassan and A. Abraham, "Modeling insurance fraud detection using imbalanced data classification," in *Advances in Intelligent Systems and Computing*, 2016. doi: 10.1007/978-3-319-27400-3_11.
7. P. Ashok and A. S. Durge, "Fraud Detection and Prevention in Healthcare Insurance Claims Using Machine Learning Regression Models," in 2025 International Conference on Data Science and Business Systems, ICDSBS 2025, 2025. doi: 10.1109/ICDSBS63635.2025.11031751.
8. P. C. Shekhar, "Testing For The Unexpected: Ensuring Insurance System Stability During Covid-19," *J. Artif. Intell. Mach. Learn. Data Sci.*, vol. 1, no. 1, pp. 1–15, November, 2022, doi: doi.org/10.51219/JAIMLD/Chandra-shekhar-pareek/375.
9. S. Thiprungsri and M. Vasarhelyi, "Cluster Analysis for Anomaly Detection in Accounting Data: An Audit Approach," *Int. J. Digit. Account. Res.*, vol. 11, 2011, doi: 10.4192/1577-8517-v11_4.
10. B. Mohanty, "Role of artificial intelligence in financial fraud detection," 2023.
11. A. Warriar and K. Abhilash, "Autonomous Agentic AI for Clinical Workflow Orchestration: Self-Managing Healthcare Operations," in 2025 6th International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS), Bengaluru, India: IEEE, 2025, pp. 1450–1457, December. doi: 10.1109/ICICNIS66685.2025.11315712.
12. J. Xu, T. Yang, S. Zhuang, H. Li, and W. Lu, "AI-based financial transaction monitoring and fraud prevention with behaviour prediction," *Appl. Comput. Eng.*, 2024, doi: 10.54254/2755-2721/77/2024ma0068.
13. R. Palwe, "Adaptive human: AI decision support for high-stakes financial advice," *Int. J. Comput. Artif. Intell.*, vol. 6, no. 2, pp. 385–392, Jul. 2025, doi: 10.33545/27076571.2025.v6.i2e.226.
14. P. Adhikari, P. Hamal, and Francis Baidoo Jnr, "Impact and regulations of AI on labor markets and employment in USA," *Int. J. Sci. Res. Arch.*, 2024, doi: 10.30574/ijrsra.2024.13.1.1670.
15. B. Sharan, M. Hassan, V. D. Vani, V. H. Raj, Ginini Nijhawan, and P. P. Pawar, "Machine Learning-Based Fraud Detection System for Insurance Claims in IoT Environment," in 2024 International

- Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), 2024, pp. 1–5. doi: 10.1109/ACCAI61061.2024.10601786.
16. P. Adhikari, P. Hamal, and F. B. Jnr, "Artificial Intelligence in fraud detection: Revolutionizing financial security," *Int. J. Sci. Res. Arch.*, vol. 13, no. 01, pp. 1457–1472, 2024.
17. P. Chandra Shekhar, "Next-Gen Test Automation in Life Insurance: Self-Healing Frameworks," *Int. J. Sci. Res. Eng. Manag.*, vol. 5, no. 7, pp. 1–13, 2021, doi: 10.55041/IJSREM9554.
18. S. Farzai and A. Ghorbani, "Fraud Detection in Automobile Insurance using a Data Mining Based Approach," *Int. J. Mechatronics, Electr. Comput. Technol.*, 2018.
19. D. Vineela*, P. Swathi, T. Sritha, and K. Ashesh, "Fraud Detection in Health Insurance Claims using Machine Learning Algorithms," *Int. J. Recent Technol. Eng.*, 2020, doi: 10.35940/ijrte.e6485.018520.
20. S. Subudhi and S. Panigrahi, "Detection of Automobile Insurance Fraud Using Feature Selection and Data Mining Techniques," *Int. J. Rough Sets Data Anal.*, 2018, doi: 10.4018/ijrdsda.2018070101.
21. N. Duwadi and A. Sharma, "Comparative Study of Machine Learning Techniques for Insurance Fraud Detection," *Aviat. Electron. Inf. Technol. Telecommun. Electr. Control.*, 2024, doi: 10.28989/avitec.v6i2.2340.
22. H. L. Sithic and T. Balasubramanian, "Survey of Insurance Fraud Detection Using Data Mining Techniques," no. 3, pp. 62–65, 2013.
23. B. Clark, L. Mitchell, and G. Christopher, "Insurance Fraud Detection: Insights from Artificial Intelligence and Machine Learning," 2025.
24. O. A. Bello, A. Folorunso, and J. Onwuchekwa, "A comprehensive framework for strengthening USA financial cybersecurity: Integrating machine learning and AI in fraud detection systems," *Eur. J. Comput. Sci. Inf. Technol.*, 2023.
25. M. G. Kibria and M. Sevkli, "Application of Deep Learning for Credit Card Approval: A Comparison with Two Machine Learning Techniques," *Int. J. Mach. Learn. Comput.*, 2021, doi: 10.18178/ijmlc.2021.11.4.1049.
26. M. Vriscu, "Harnessing Artificial Intelligence for Risk Assessment and Fraud Detection in Insurance: A Modern Approach to Predictive Modeling," *Proc. Int. Conf. Bus. Excell.*, 2025, doi: 10.2478/picbe-2025-0179.
27. S. Ragaupathy and M. Mittal, "Next-Generation Crm In Healthcare: The Role of AI, Predictive Analytics, And Patient Journey Mapping," *Int. J. Cust. Relatsh. Manag.*, vol. 4, no. 2, pp. 1–24, July–December, 2025, doi: 10.34218/IJCRM_04_02_001.
28. D. Coals, A. John, and K. Khan, "Detecting Insurance Fraud using AI: A Case Study of Claims Processing," 2025.
29. H. Narne, "Machine Learning for Health Insurance Fraud Detection: Techniques, Insights, and Implementation Strategies," *Int. J. Res. Anal. Rev.*, 2024.
30. M. Abdul Salam, K. M. Fouad, D. L. Elbably, and S. M. Elsayed, "Federated learning model for credit card fraud detection with data balancing techniques," *Neural Comput. Appl.*, 2024, doi: 10.1007/s00521-023-09410-2.
31. S. O. Boufaida, A. Benmachiche, M. Maatallah, and C. Chemam, "An Extensive Examination of Varied Approaches in E-Learning and MOOC Research: A Thorough Overview," in *PAIS 2024 - Proceedings: 6th International Conference on Pattern Analysis and Intelligent Systems*, 2024. doi: 10.1109/PAIS62114.2024.10541129.
32. I. Soualmia, S. Maalem, A. Benmachiche, K. Rais, and M. Derdour, "Comparative Survey of AI-Driven Credit Card Fraud Detection: Machine Learning, Deep Learning and Hybrid Systems," in *2025 International Conference on Networking and Advanced Systems (ICNAS)*, IEEE, Oct. 2025, pp. 1–9. doi: 10.1109/ICNAS68168.2025.11298125.
33. S. K. Madishetty, "Cyber Resilience and DevOps in Operating Rooms: Securing Connected Embedded Medical Devices in High Risk Clinical Environments," *J. Electr. Syst.*, vol. 19, no. 3, pp. 244–253, Jan. 2024, doi: 10.52783/jes.9597.
34. R. Gupta, "Artificial Intelligence (AI) in Insurance: A Futuristic Approach," *Rev. Ref. Res. Journal*, 2020.
35. R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," *Stat. Sci.*, vol. 17, no. 3, pp. 235–255, 2002, doi: 10.1214/ss/1042727940.
36. K. Crawford and T. Paglen, "Excavating AI: the politics of images in machine learning training sets," *AI Soc.*, 2021, doi: 10.1007/s00146-021-01162-8.
37. I. I. J. Rifka Alkhilyatul Ma'rifat, I Made Suraharta, "Artificial Intelligence In Insurance Processes: Fraud

- Detection And Risk Mitigation,” vol. 2, pp. 306–312, 2024.
38. V. Priya, R. S. Priya, and D. S. Priya, “An Intelligent Deep Learning Framework for Scalable Insurance Fraud Detection and Risk Assessment,” in 2026 4th International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), 2026, pp. 172–179. doi: 10.1109/ICSSAS68835.2026.11559352.
 39. S. Peykani and E. Kugu, “Explainable Artificial Intelligence (XAI) In Insurance Fraud Detection,” in 2026 5th International Informatics and Software Engineering Conference (IISEC), 2026, pp. 537–542. doi: 10.1109/IISEC69317.2026.11418497.
 40. R. Agarwal, D. Kalsi, P. Jain, P. Gupta, and R. Goel, “Car Insurance Fraud Detection using Machine Learning Models,” in 2025 International Conference on Next Generation Information System Engineering (NGISE), 2025, pp. 1–8. doi: 10.1109/NGISE64126.2025.11085234.
 41. P. K. Gupta, R. Bhatnagar, S. Tyagi, A. Jain, A. Panwar, and A. K. Dubey, “Machine Learning Algorithms for Auto Insurance Fraud Detection: Comparative Study,” in 2024 IEEE 1st International Conference on Green Industrial Electronics and Sustainable Technologies, GIEST 2024, 2024. doi: 10.1109/GIEST62955.2024.10959939.
 42. K. P. Rijanto, D. A. Putri, P. Calvin, I. S. Edbert, and D. Suhartono, “Machine Learning Algorithms with Oversampling Methods for Automobile Insurance Fraud Detection,” in 2023 IEEE 21st Student Conference on Research and Development (SCoReD), 2023, pp. 138–143. doi: 10.1109/SCoReD60679.2023.10563582.
 43. B. K. Sethi, D. Singh, and P. K. Sarangi, “Medical Insurance Fraud Detection Based on Block Chain and Deep Learning Approach,” in 2022 International Conference on Disruptive Technologies for Multi-Disciplinary Research and Applications (CENTCON), 2022, pp. 103–106. doi: 10.1109/CENTCON56610.2022.10051253.