International Journal of Leading Research Publication (IJLRP)

E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

AI-Powered Fraud Detection in Insurance and Banking

Kranthi Kumar Asike Parameshwa

Lamar University, College of Business

Abstract:
This paper focuses on Artificial Intelligence (AI) to detect fraud in the banking and insurance industry. Due to the rapid development of online financial services, fraud cases, including identity theft, credit card fraud, and fake insurance claims are becoming smarter. The old rule-based systems are no longer adequate to identify the changing trends in fraud and there is need to have more dynamic and modernized solutions. Machine learning, deep learning, and data analytics are AI-based methods that assist in detecting and preventing fraud with considerable improvements. The paper discusses the different AI models that are applied in the detection of fraud and they include supervised and unsupervised learning algorithm, anomaly detection and neural networks. These methods allow to track in real time transaction tracking, detect suspicious patterns, and decrease false positives. AI has been popular in the banking industry in detection of credit card frauds, anti-money laundering, and identity checks. AI is used in the insurance sector to detect customer frauds, customer behavior, and to enhance the risk assessment procedure. Although it has benefits, AI-based fraud detection has issues including data privacy, model's interpretability and quality of dataset adversities. The research outlines these weaknesses in the context of explaining the possible future trends, such as explainable AI and the incorporation of new technologies, such as blockchain. In general, AI is essential in improving the efficacy, precision, as well as dependability of fraud detection mechanisms in contemporary fiscal conditions.

Keywords: Artificial Intelligence (AI), Fraud Detection, Machine Learning (ML), Deep Learning (DL), Banking Security, Insurance Fraud, Anomaly Detection, Data Analytics, Financial Crime, Risk Assessment.

1. Introduction

The issue of fraud in the banking and insurance sectors has grown into a significant problem, especially with the active growth of online banking and other online financial opportunities (Hafez et al., 2025; View of Artificial Intelligence and Fraud Detection: An Overview, n.d.; Ahmad, 2025). The rising trend of mobile banking, electronic payments, and online insurance systems has offered fraudsters new ways of abusing the weak points of the systems (View of Artificial Intelligence in Insurance: Leveraging machine learning for fraud detection and risk evaluation, n.d.; Ali et al., 2022). This has led to massive losses of money, tarnished images and regulatory difficulties in the hands of financial institutions, which engage in fraudulent practices like identity theft, credit card fraud, money laundering as well as fake insurance claims (Zarifis et al., 2019; Noreen et al., 2023). Historically, fraud detection systems have been based on rule-based systems, in which a set of rules and thresholds are set to detect suspicious behavior. These systems, though effective in identifying the known pattern of fraud, are not as efficient as the new and changing fraud patterns (Narang et al., 2024; Gyau et al., 2024). Further, systems based on rules in most instances produce a substantial number of false positives, not only raising operational costs but also negatively affecting customer experience. Artificial Intelligence (AI) has become an influential tool in the past few years that has contributed to boosting the capacity of detecting fraud (Hafez et al., 2025; Pang et al., 2021). AI-based systems are designed to operate on sophisticated algorithms including machine learning, deep learning, and data analytics to detect complex trends that are related to fraudulent activities using large

amounts of data. In contrast to the traditional systems, AI models do not have to stop learning as new data is always available, and thus they can identify new fraud patterns and increase the accuracy of their detection with time. The application of AI in the banking industry is common in credit card fraud detection, anti-money laundering, and biometric authentication (Ahmad, 2025; Noreen et al., 2023). Likewise, AI is also essential in the insurance sector to identify fraudulent cases, customer behavior, as well as enhance risk evaluation activities (View of Artificial Intelligence in Insurance: Leveraging machine learning for fraud detection and risk evaluation, n.d.; Ali et al., 2022). These applications do not only increase security, but also make operations more seamless and less costly.In spite of all these benefits, AI models have also been challenged when it comes to the detection of frauds with issues such as data privacy, compliance with various regulations, and the complexity of AI models (Zarifis et al., 2019; Gyau et al., 2024; Pang et al., 2021). Thus, the advantages and disadvantages of AI-powered systems detecting fraud should be evaluated critically. The objective of this paper is to give an overview of AI implementation in the banking and insurance sectors in detecting fraud. It examines the major methods, applications, advantages, issues, and future tendencies and emphasizes the revolutionary nature of AI on the financial systems nowadays.

2. Literature Review

Recent studies have shown the significance of Artificial Intelligence (AI) in the detection of fraud. A comprehensive review of the significance of AI-based models in the detection of credit card fraud has been presented by Hafez et al. (2025). In the same direction, the significance of the use of machine learning and ensemble models has been highlighted by researchers like Ali et al. (2022) and Talukder et al. (2024) for the improvement of the accuracy of the detection of credit card fraud. Moreover, the significance of the use of deep learning models has been presented by Pang et al. (2021) for the detection of anomalies. Studies like Ahmad (2025) and Noreen et al. (2023) have explored the applications of AI in the banking sector. In the digital banking environment, the significance of the use of AI for the improvement of the detection of fraud has been shown. In the insurance field, various studies have shown the effectiveness of AI techniques like machine learning and natural language processing in the detection of fraudulent claims. Zarifis et al. (2019) presented the transformation of insurance business models by applying AI. In addition, various studies have been conducted on the applications of AI in the insurance field. In the insurance field, the applications of data-driven approaches have been presented to detect fraudulent claims. Furthermore, various studies have been conducted to apply the frameworks of anomaly detection systems and hybrid models of AI to overcome the challenges of data imbalance, drift, and attacks. In addition, the applications of explainable AI have been presented to increase the trust of the system. In the insurance field, various studies have been conducted to analyze the applications of AI systems in financial services and profitability. In the insurance field, the applications of AI systems have been presented to detect fraudulent claims. Despite the above advancements, several challenges persist. These challenges include data privacy concerns, interpretability of the models, and the dynamics of fraud schemes. Al-Daoud and Abu-AlSondos (2025) emphasized the requirement for strong and flexible AI frameworks to overcome the above challenges. In conclusion, the literature review indicates that the use of AI-based systems for fraud detection is beneficial due to the accuracy, adaptability, and scalability of the systems.

3. Methodology

The methodology section provides an outline of the approach and framework that was employed in conducting this study to understand the role played by Artificial Intelligence in fraud detection in banking and insurance industries. This section provides an outline of how data was collected, analyzed, and interpreted to ensure that a clear and comprehensive understanding of AI techniques, applications, and results was established. The approach employed in this study provides a clear foundation for the subsequent discussion regarding AI techniques, applications, and results, as it ensures that the study was conducted in an effective manner to achieve this objective.

3.1 Research Design

The purpose of the present study is to conduct a qualitative and analytical research investigation aimed at exploring the application and effectiveness of Artificial Intelligence (AI) in the detection of fraud cases in the banking and insurance industries. The present research aims at exploring the various techniques of AI, the practical implementation of these techniques, and the overall efficiency of the techniques in the detection of fraud cases. A structured approach has been adopted to conduct the research, which includes the overall analysis of the literature, case studies, and practical implementation of AI techniques. The present research aims at critically evaluating the AI models, including machine learning, deep learning, anomaly detection, and natural language processing, with the aim of highlighting the potential of AI techniques.

3.2 Data Collection

For the purpose of data collection for this particular study, the researcher depends on secondary sources of data. These include journal articles, conference publications, industry reports, and case studies of various banking and insurance institutions. These sources of data are reliable and provide quality information on the application of various AI techniques and the results observed. Additionally, the researcher accesses various datasets and analyses of various AI models to understand the performance parameters of the models and the applicability of the models to various financial institutions. This is due to the fact that the researcher depends on secondary sources of data, which provide a wide range of data on the subject. This helps the researcher to provide a holistic view of the application of AI techniques for the purpose of fraud detection. No primary data collection was conducted for the purpose of the research.

3.3 Data Analysis

The data thus obtained is analyzed through a structured three-phase approach. In the first phase, the different AI technologies presently employed in fraud detection are identified and grouped. These include supervised and unsupervised machine learning models, deep learning models, anomaly detection models, and natural language processing models. Each of these models is assessed based on their functionality, advantages, and disadvantages, along with their practicality in real-world banking and insurance scenarios. In the second phase, a comparative analysis is carried out between AI-based models and traditional rule-based models for fraud detection. Various key performance indicators are taken into consideration to evaluate the effectiveness and efficiency of AI-based models. In the last phase, a real-world case study analysis is performed to evaluate the effectiveness of AI models in fraud detection. In such case studies, real-world scenarios are considered to evaluate the effectiveness of AI models in improving detection rates, reducing costs, and improving customer trust.

3.4 Limitation

Despite the exhaustive nature of the research, there are certain limitations. To begin with, the fact that the research has relied on secondary data implies that the analysis has been based on the availability of the data. There might be certain emerging techniques or unique applications of AI, which have not yet been documented. Moreover, the fact that the research has not relied on any primary experimentation implies that there might be difficulties in performing any empirical testing of the performance of the AI models. Another aspect of the research is the fact that the landscape of financial fraud as well as AI models is constantly changing, which implies that the findings of the research might have to be periodically updated. Additionally, there are aspects of data privacy, which might have a bearing on the applicability of certain AI models.

Table 1. Summary of Data Sources and Analysis Approach
In this table, each step of the research, along with the sources of data and the importance of each step in analyzing the AI techniques used in fraud detection, is provided. This will give the readers a clear idea about the research methodology followed in this research**.**

Phase / Step	Description	Purpose / Objective
Data Collection	Peer-reviewed journals, conference papers, industry reports, case studies	To gather validated information on AI techniques and applications
Identification of AI Techniques	Machine learning, deep learning, anomaly detection, NLP	To categorize methods used in fraud detection
Comparative Analysis	Compare AI vs traditional rule-based systems	To evaluate effectiveness, accuracy, and efficiency
Case Study Evaluation	Real-world banking and insurance applications	To assess practical outcomes and system performance

4. AI Techniques for Fraud Detection

Significantly, AI has revolutionized fraud detection through the incorporation of new computational methods that can process large-scale financial data with precision and speed. Financial institutions and insurance companies can easily recognize complex fraud patterns through these methods, which can detect anomalies in real-time while responding to changing fraud behaviors. The main AI methods used in fraud detection are machine learning, deep learning, anomaly detection, natural language processing, and hybrids**.**

4.1 Machine Learning Techniques

The contemporary fraud detection systems are based on machine learning (ML). It helps systems to learn out of the past transactional data and determine patterns that relate to fraudulent activity. The ML methods can be divided into unsupervised and supervised learning. The models of supervised learning are trained on labeled samples on which transactions are categorized as either being fraudulent or legitimate. Widely used algorithms would be logistic regression, decision trees, support vector machines (SVM) and ensemble algorithms like random forests and gradient boosting machine. They are also effective and widely used in credit card fraud detection systems to detect known patterns of fraud. The strong accuracy of the supervised learning, in the case of sufficient labeled data, is one of the key virtues of the method. It however encounters the problems like imbalance in classes with fraudulent transactions being a very insignificant fraction of the data. Methods to deal with this problem include oversampling, under sampling and synthetic data generation (e.g. SMOTE). On the other hand, the unsupervised learning methods do not use labelled data. The algorithms employed are k-means clustering and hierarchical clustering to cluster similar transactions and establish outliers. These techniques can be utilized in identifying frauds that are new or unknown. They can however produce more false positives than supervised methods.

4.2 Deep Learning Approaches

Deep learning (DL) is an extension of the conventional machine learning, which uses multi-layered neural networks to represent the complexity of the relationship within data. It is especially useful to operate with large-scale and high-dimensional data, which is typical of financial systems. The model in question is an Artificial Neural Network (ANNs) with the nonlinear associations of input characteristics and the outcomes of the fraud. Although CNNs have been associated with image processing, there has been an adoption of CNNs to structured financial data to extract features. Recurrent Neural Networks (RNNs) are particularly the Long Short-Term Memory (LSTM) networks that are very effective in the analysis of sequence data including transaction histories. Features that are relevant to raw data may be extracted automatically due to deep learning models and need not be engineered manually. This can be effective

especially in the area of fraud where concealed patterns may not be easily detected through the conventional means. Although they have their benefits, deep learning models are very demanding in terms of data and computation. Also, they are black box in nature, and thus hard to interpret which in cases of regulated industries such as banking and insurance can be an issue.

4.3 Anomaly Detection

Anomaly detection is also important in detection of fraudulence which is an irregular operation. In contrast to supervised learning, fraud detection is aimed at identifying suspicious trends as opposed to using predefined labels of fraud. Isolation forests, one-class support vector machines, and autoencoders are some of the commonly used techniques in detection of anomalies. Such models set a standard of normal behavior of transactions and put abnormalities to the fore as possible fraud. As an example, high-value transaction that is made suddenly with unusual geographic location can be observed as an anomaly. This is very effective especially in identifying the zero-day fraud attacks and new trends of fraud that have never been recorded before. Real-time fraud detection systems have been extensively applied in anomaly detection because they are able to detect anything suspicious in real-time. Nonetheless, it might need to be fine-tuned in order to decrease the instances of false positives and enhance reliability. Natural language processing (NLP) involves the computational processing of languages through algorithms.

4.4 Natural Language Processing

NLP refers to the process of processing languages with algorithms. A wide field of application of NLP in fraud detection is also in the insurance industry where a lot of information exists in the form of unstructured data. The textual data that can be analyzed using NLP techniques includes claim forms, customer complaints, emails, and investigation reports. Stunning techniques in NLP models, including tokenization, sentiment analysis, named entity recognition, and text classification, can be used to derive valuable information in text information. As one example, missing consistency in the description of claims, exaggerated language, or repetition in fraudulent claims can be detected with the help of NLP. Moreover, it is possible to use NLP alongside machine learning models to enhance the accuracy of fraud detection based on both the structured and unstructured data. Such a combined method has the positive impact on the effectiveness of the fraud detection systems.

4.5 Hybrid AI Models

Multi-technique AI models are used where two or more techniques can be used to utilize their forces and reduce their weaknesses. As an example, a fraud detection system can apply supervised learning to classify it, anomaly detection to detect patterns of unknown fraud, and NLP to examine textual evidence. These combined systems have a more detailed method of fraud detection since they touch on various facets of fraudulent behavior. Complex environments with dynamic and multifaceted fraud patterns are the most effective with hybrid models. Besides, hybrid options enhance system performance in terms of robustness, ease of scale, and flexibility, which make them applicable to large-scale financial systems. Numerous banking and insurance fraud detection systems developed today are founded on hybrid AI architectures

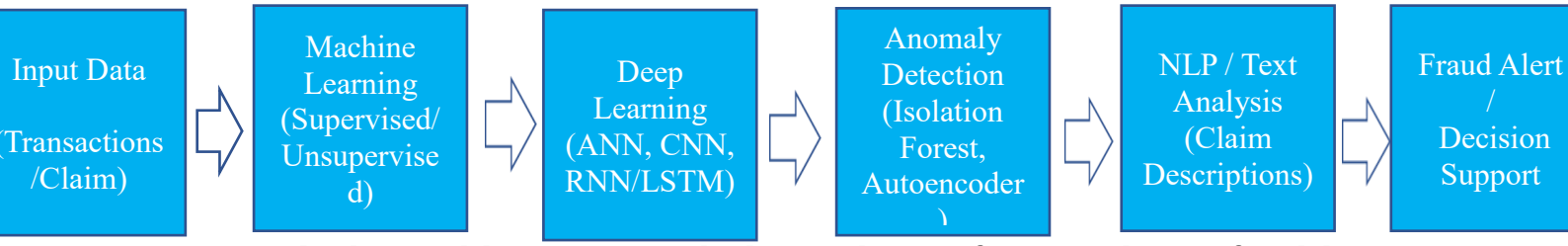

Figure 1. Hybrid AI model integrating multiple AI techniques for comprehensive fraud detection in banking and insurance sectors.2

Figure 1 depicts the architecture of a hybrid AI model, which includes machine learning, deep learning, anomaly detection, and natural language processing techniques for detecting fraudulent activities. The flowchart in Figure 2 explains how data inputs are processed using different AI techniques for more accurate detection and identification of anomalies and fraudulent activities. The final result is a fraud detection decision, which explains how different AI techniques are used in practice for fraud detection.

Table 2. Summary of AI Techniques for Fraud Detection

In Table 2, the prominent AI techniques used in fraud detection have been provided, along with the type, usage, and advantages of each technique.

Technique	Type	Use Case	Advantage
Machine Learning (ML)	Supervised / Unsupervised	Credit card fraud, policy fraud detection	High accuracy for known patterns; adaptable with new data
Deep Learning (DL)	Neural Networks	Sequential transaction analysis, anomaly detection	Automatic feature extraction; handles large, complex datasets
Anomaly Detection	Unsupervised	Zero-day fraud detection, real-time monitoring	Detects previously unknown fraud; instant alerts
Natural Language Processing (NLP)	Textual Analysis	Insurance claim analysis, customer emails	Identifies inconsistencies in text; improves claim review
Hybrid AI Models	Integrated Approach	Multi-channel fraud detection	Combines strengths of different techniques; higher robustness

5. Applications in Banking Sector

One of the first areas in which Artificial Intelligence (AI) has been used to detect fraud is in the banking sector, where banks are now dealing with more advanced and more intensive fraud cases. With the help of AI-powered systems, banks can identify anomalies, thwart losses, and comply with regulations because they can process the data on the scale of transactions in real time. Credit card fraud detection is one of the most widespread applications where AI algorithms or algorithms track transactional patterns and spending patterns, as well as geolocation to determine problematic actions. Machine learning algorithms, including gradient boosting and random forests, are able to identify abnormal purchases that do not align with an accepted customer behavior therefore minimizing financial losses and false alarms. Anti-money laundering (AML) is another important one. Regulators make banks monitor and report suspicious financial practices. AI systems process a lot of connections of transactions, detect suspicious fund transfers, and predict possible money laundering patterns. Methods like anomaly detection and deep learning enable banks to trace multi-step and cross-border transaction which could be an indication of illicit activities and thus are sometimes not detected by traditional rule-based systems. AI has also transformed the process of identity verification and authentication. Facial recognition, fingerprint identification, and behavioral analysis are biometric technologies that are becoming part of banking in the effort to avoid access by unauthorized individuals and identity theft. AI models have the ability to identify anomalous logging behaviors, unusual activity of a device or abnormal timing of transactions, which goes beyond passwords and OTPs, offering an extra security measure. Another important application is real

time monitoring of transactions. AI applications constantly compare every transaction to historical data and patterns of fraud, which sends immediate warnings of any suspicious behavior. This is especially useful on the digital and mobile banking platforms where the transactions take place at an extremely high speed and magnitude. Additionally, predictive modeling can be used to enable the banks to identify high-risk accounts in advance and thwart any fraud before it happens. A number of major banks have stated that there was significant improvement when they used AI-based fraud detection systems. As an illustration, AI has facilitated quicker identification of credit card fraud, enhanced the precision of monitoring transactions, and lower operational expenses that has to be incurred in processing the transactions manually. The combination of various AI methods can help banks to have a more holistic and flexible method of fraud detection, which eventually increases the level of security and customer confidence.

6. Uses in Insurance Sector

On an annual basis, the insurance industry is incurring huge financial losses because of fraudulent claims, false documentation, policy manipulation and similar practices. The Artificial Intelligence (AI) has proved to be a potent weapon against these obstacles, allowing insurers to identify, deter and investigate cases of frauds very effectively. Fraudulent claim identification belongs to the top utilization of AI in the insurance industry. By training machine learning models using historical claims data, it is possible to identify patterns and anomalies in those claims that point to the possibility of fraudulent behavior. Such models consider several claim characteristics such as claim amount, type, claimant history, and claim timing in order to establish the risk probability of fraud. Natural Language Processing (NLP) has gained value especially in the analysis of unstructured textual data, including description of claims, customer emails, and reports of investigations. The NLP algorithms identify inconsistencies, strange use of words or repetition of language patterns which might portray a fraud motive. As an illustration, a claimant that makes repetitive or exaggerated claims in different claims may be noted in order to have additional investigation. The integration of NLP and structured data analysis improves the performance of fraud detection and reduces the false positives, optimizing the efficiency of operations. The other important use is in processing of images and documents using computer vision method. Photos, scans, or digital documents are frequently provided in claims submissions in such sectors as auto, health, and property insurance. Image recognition algorithms that can be executed using AI can be used to automatically analyze the damages on vehicles or property or medical records to identify any difference between the reported claim and evidence on the ground. This will minimize the reliance on manual inspection and speed up the processing of claims. Risk assessment and underwriting include the use of AI as well. Predictive models are used to analyze customer information, the past records of claims and external information to determine the likelihood of a fraudulent activity and subsequently issue policies. Such proactive strategy will assist the insurance firms to reduce their exposure to risky customers and be able to customize the cover policy as needed. Moreover, AI allows tracking claims in real time. There are systems to constantly analyze the data that enters it and the transactions with policyholders so that to identify suspicious patterns immediately. Insurance companies can establish multi-layered fraud detection systems with the help of various AI methods, such as machine learning, deep learning, anomaly detection, and NLP. The outcome is higher faster and more accurate fraud detection, cost reduction in the operations and customer satisfaction and loyalty.

Table 3. AI Techniques Across Banking and Insurance Applications

Table 3 represents a comparative overview of the major techniques of AI applied to the banking and insurance sectors. It describes the specific application of each technique, such as credit card fraud detection, anti-money laundering, claim analysis, anomaly detection, and the major benefits of applying each of the techniques to the sectors. This will help readers understand the application of various

techniques of AI and the major advantages of applying them to the sectors for the detection of fraudulent activities.

AI Technique	Sector	Application	Key Benefit
Machine Learning (ML)	Banking	Credit card fraud detection, AML	High detection accuracy, adaptable
Machine Learning (ML)	Insurance	Claim analysis, policy fraud detection	Identifies suspicious claims efficiently
Deep Learning (DL)	Banking	Sequential transaction monitoring	Automatic feature extraction, handles large data
Deep Learning (DL)	Insurance	Claim pattern recognition, anomaly detection	Detects complex fraudulent patterns
Anomaly Detection	Banking	Real-time transaction alerts	Identifies unknown fraud patterns
Anomaly Detection	Insurance	Unusual claim detection	Detects emerging fraud
Natural Language Processing (NLP)	Insurance	Textual claim analysis, emails	Detects inconsistencies and suspicious intent
Hybrid Models	Both	Multi-channel fraud detection	Combines strengths of multiple techniques

7. Benefits and Challenges of AI in Fraud Detection

The application of Artificial Intelligence (AI) in fraud detection in banking and insurance industries has shown significant advantages. The first advantage is that it improves accuracy in fraud detection, as it can process large amounts of data to detect complex patterns that could be an indicator of fraud. This improves efficiency in fraud detection, as there will be fewer false positives. The second advantage is that AI improves cost efficiency, as it automates processes that were previously done manually. The third advantage is that AI improves efficiency in fraud detection, as it can monitor activities in real-time, thus enabling instant fraud detection and preventive measures to be taken. However, the application of AI is also accompanied by some challenges. First and foremost, the quality and availability of data are essential considerations in the application of AI systems, as poor quality and availability of data may have a negative impact on the performance of the models. Second, the issue of data privacy is a significant concern in the application of AI systems, particularly in the handling of sensitive financial and personal data. Third, the issue of interpretability is a significant concern in the application of AI systems, particularly in the application of deep learning models, as they are considered “black boxes” and may be difficult to interpret and communicate to relevant stakeholders and regulators. Finally, fraudsters are continually evolving sophisticated techniques and methods, and therefore, the application of AI systems must be continually updated and maintained. By carefully weighing the advantages and disadvantages of the application of AI systems in the prevention of fraud, financial institutions and insurance companies may be able to optimize the application of AI systems in the prevention of fraud.

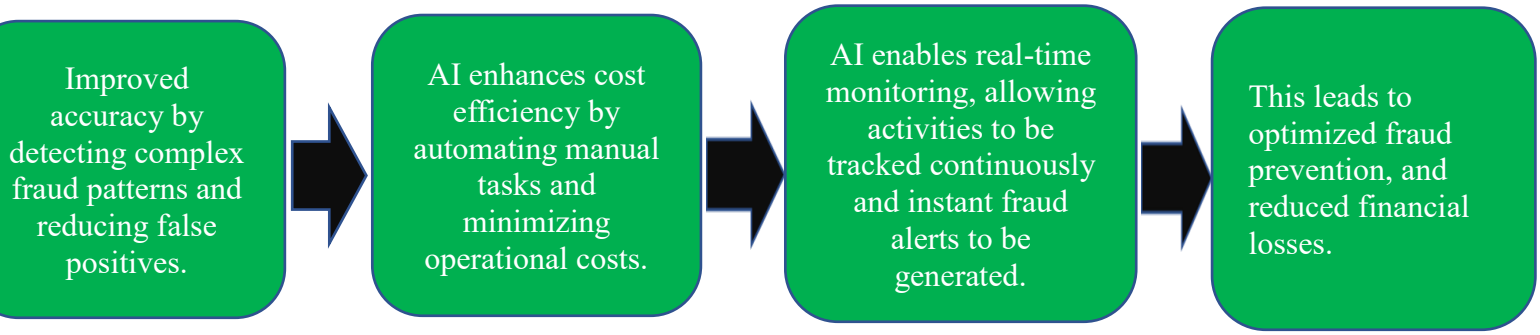

Figure 2. Benefits of AI in Fraud Detection

The given figure illustrates the core advantages of using AI in the fight against fraud in banking and insurance industries. It emphasizes the way AI will improve accuracy by identifying sophisticated fraud patterns and minimizing false positive, operational efficiency of automation, real-time monitoring to provide instant notifications, and eventually result into optimal fraud prevention and decreased monetary losses.

8. Discussion

The adoption of Artificial Intelligence (AI) in fraud detection has revolutionized the banking, as well as insurance, industries and offered superior instruments to detect, prevent, and counter fraudulent activities. AI methods such as machine learning, deep learning, anomaly detection, and natural language processing have proven very accurate in identifying complex cases of fraud that rule-based systems are often unable to detect. In real practice, AI, in addition to increasing detection rates, is proven to lower costs in operation, improve customer confidence, and provide the opportunity to monitor financial transactions and insurance claims in real time. Nevertheless, the discussion also identifies some challenges that institutions can struggle with when applying AI. The quality of data, privacy, compliance with the regulations, and interpretability of the model are crucial points that should be handled. Moreover, as fraud is dynamic, AI models should be constantly adapted and updated, as they need to be effective. Regardless of these obstacles, the implementation of hybrid AI solutions and the incorporation of several methods has a decent future of more resistant and more adaptive fraud detection systems. In general, the available findings indicate that AI can be used as a preventive and investigative tool, allowing institutions to deal with fraud proactively enhancing efficiency and reliability. It is discussed that the balanced attitude should be taken exploiting the opportunities of AI, but also eliminating possible drawbacks with strict control over governance, transparency and ethical data standards.

9. Conclusion

AI has become a revolutionary solution to fight fraud within a banking and insurance business. Financial institutions will be able to identify the existence of complex cases of fraud more effectively and efficiently by using advanced technologies like machine learning, deep learning, anomaly detection, and natural language processing. Operating AI allows real-time monitoring, adaptive learning, and economical operations, which greatly improves the strategies of fraud prevention. Although it has its benefits, issues pertaining to data quality, privacy, compliance, and interpretability of the model should be tackled to achieve responsible and effective utilization of AI. The paper highlights that the most effective way of detecting fraud is by using a set of several AI in conjunction with robust governance and regular system upgrades. Finally, AI enhances security and operational efficiency as well as fosters confidence in customers due to the ability to prevent fraud proactively and intelligently. With the prevailing changes in the patterns of fraud, acceptance and development of AI-based systems will be necessary to ensure financial transparency and sustainability across the banking and insurance industries.

REFERENCES:

1. Hafez, I. Y., Hafez, A. Y., Saleh, A., El-Mageed, A. a. A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data*, *12*(1). https://doi.org/10.1186/s40537-024-01048-8
2. *View of Artificial Intelligence and Fraud Detection: An Overview*. (n.d.). https://jurnal.upnyk.ac.id/index.php/jmar/article/view/16268/7527
3. Ahmad, E. (2025). AI-Powered Fraud Detection and Prevention in Banking. *Journal of Informatics Education and Research*, *5*(2). https://doi.org/10.52783/jier.v5i2.2657
4. *View of Artificial Intelligence in Insurance: Leveraging machine learning for fraud detection and risk evaluation*. (n.d.). https://www.ijisae.org/index.php/IJISAE/article/view/7847/6866

5. Ali, A., Razak, S. A., Othman, S. H., Eisa, T. a. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial Fraud Detection Based on Machine Learning: A Systematic Literature review. *Applied Sciences*, *12*(19), 9637. https://doi.org/10.3390/app12199637
6. Zarifis, A., Holland, C. P., & Milne, A. (2019). Evaluating the impact of AI on insurance: the four emerging AI- and data-driven business models. *Emerald Open Research*, *1*(1). https://doi.org/10.1108/eor-01-2023-0001
7. Noreen, U., Shafique, A., Ahmed, Z., & Ashfaq, M. (2023). Banking 4.0: Artificial Intelligence (AI) in Banking Industry & Consumer's Perspective. *Sustainability*, *15*(4), 3682. https://doi.org/10.3390/su15043682
8. Narang, A., Vashisht, P., & Bajaj, S. B. (2024). Artificial intelligence in banking and finance. *International Journal of Innovative Research in Computer Science & Technology*, *12*(2), 130–134. https://doi.org/10.55524/ijircst.2024.12.2.23
9. Gyau, E. B., Appiah, M., Gyamfi, B. A., Achie, T., & Naeem, M. A. (2024). Transforming banking: Examining the role of AI technology innovation in boosting banks financial performance. *International Review of Financial Analysis*, *96*, 103700. https://doi.org/10.1016/j.irfa.2024.103700
10. Pang, G., Shen, C., Cao, L., & Van Den Hengel, A. (2021). Deep learning for anomaly detection. *ACM Computing Surveys*, *54*(2), 1–38. https://doi.org/10.1145/3439950
11. Al-Daoud, K. I., & Abu-AlSondos, I. A. (2025). Robust AI for Financial Fraud Detection in the GCC: a hybrid framework for imbalance, drift, and adversarial threats. *Journal of Theoretical and Applied Electronic Commerce Research*, *20*(2), 121. https://doi.org/10.3390/jtaer20020121
12. *View of EFFECT OF AI-POWERED FRAUD DETECTION SYSTEMS ON PROFITABILITY OF FINANCIAL INSTITUTIONS*. (n.d.). https://www.jmsrr.com/index.php/Journal/article/view/182/158
13. *View of The Impact of Artificial intelligence on fraud detection in Digital Banking: An Empirical study*. (n.d.). https://jier.org/index.php/journal/article/view/3936/3111
14. *View of Fraud Detection in Banking: A Deep Learning Approach with Explainable AI | Journal of Soft Computing Paradigm*. (n.d.). https://irojournals.com/jscp/article/view/1628/1470
15. *View of AI-Driven Fraud Detections in Financial Institutions: A Comprehensive study*. (n.d.). https://al-kindipublisher.com/index.php/jcsts/article/view/8687/7383
16. Islam, M. S., & Rahman, N. (2025). AI-Driven Fraud Detections in Financial Institutions: A Comprehensive study. *Journal of Computer Science and Technology Studies*, *7*(1), 100–112. https://doi.org/10.32996/jcsts.2025.7.1.8
17. *View of AI in Financial Services: Fraud Detection and Risk Management*. (n.d.). https://metall-mater-eng.com/index.php/home/article/view/1335/718
18. *View of Prediction of Insurance Fraud Detection using Machine Learning Algorithms*. (n.d.). https://publications.muet.edu.pk/index.php/muetrj/article/view/2348/566
19. *View of Leveraging AI-Driven Anomaly Detection for Fraud Prevention in annuities and Insurance Platforms: A Comprehensive Framework for Regulatory-Compliant Implementation*. (n.d.). https://al-kindipublishers.org/index.php/jcsts/article/view/11239/9993
20. Talukder, M. A., Khalid, M., & Uddin, M. A. (2024). An integrated multistage ensemble machine learning model for fraudulent transaction detection. *Journal of Big Data*, *11*(1). https://doi.org/10.1186/s40537-024-00996-5