Vol 4, Issue 7, 2021 **Impact Factor: 2.58** DOI: https://doi.org/10.31426/ijamsr.2021.4.7.4513

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Impact of Artificial Intelligence on Banking Fraud Detection

Alok Gupta

Assistant Professor, Department of Financial Studies,
V.B.S. Purvanchal University, Jaunpur, U.P.

Email Id: alokmfc76@gmail.com

A B S T R A C T

Increasing numbers of fraudulent activities have been observed inside the banking sector as a direct consequence of the proliferation of digital banking and online transactions. It is getting increasingly difficult for traditional methods of fraud detection to keep up with the ever-evolving dangers. Using information obtained from the Scopus database, this study does a bibliometric analysis, which results in the production of 66 documents. After the year 2019, India emerged as the country with the highest number of citations, accounting for 64 percent of the documents that were published. Immediately after the beginning of the Covid-19 epidemic, there was a discernible increase in the amount of interest in research. According to the findings of the investigation, artificial intelligence-based fraud detection solutions perform noticeably better than conventional approaches. The findings provide very useful insights that can be used to construct frameworks for artificial intelligence-driven fraud detection in banking.

Keywords: Banking Fraud Detection, Artificial Intelligence

INTRODUCTION

The banking industry has a growing fraud problem. This issue threatens banks and customers. As technology advances, so have fraudsters' strategies, making previous fraud detection approaches obsolete. AI has great potential in fighting fraud. Financial institutions like banks have used cutting-edge technology to bolster their defenses in response to rising threats. AI, a field of computer science that lets computers learn and do human activities, is changing how banks identify and prevent fraud. It can uncover hidden patterns, evaluate massive data, and make immediate judgments. Machine learning, a subfield of AI, lets computers learn from their experiences and improve without human involvement. Fraud has quickly growing tactics and massive data complexity; AI can identify and minimize this. These traits make AI ideal for this position.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

This introduction will focus on how AI is affecting banking fraud detection. We'll focus on its real-time data analysis, threat adaptation, and false positive reduction. It will also examine how neural networks, machine learning, and NLP are combating financial crime. Finally, it will discuss the myriad issues that may arise from employing AI to identify fraud, such as data privacy, regulatory compliance, and hostile assaults.

The Growing Need for AI in Fraud Detection

Fraud is extremely common in the banking business because it handles significant quantities of money and sensitive data. Many varieties of fraud exist, including identity theft, account takeovers, transaction fraud, and money laundering. Digital banking and online financial services have become more popular, which has led to more sophisticated fraud that exploits new technologies. Rule-based fraud detection systems have worked before. Predetermined criteria separate questionable transactions from normal ones in these systems. However, these systems struggle to keep up with the growing complexity and scope of fraud schemes. Fraudsters constantly innovate and exploit system flaws. Meanwhile, legitimate consumers' behaviours are changing, making it hard to tell fraud from actual activity.

AI helps financial organizations move from reactive to proactive fraud detection. By learning from past and present transactions, artificial intelligence systems adapt to new behavior patterns rather than following static rules that may be evaded. Artificial intelligence models can spot slight transaction data irregularities that traditional systems miss. AI models can detect tiny changes, making this ability to develop vital to detecting new fraud.

Real-Time Fraud Detection and Anomaly Detection

Real-time data analysis is a significant advantage of AI for fraud detection. Banking transactions occur in milliseconds, thus real-time fraud detection and prevention are essential to reducing financial losses and maintaining consumer confidence. AI can analyze several factors and interpret enormous datasets in real time. These include the overall amount spent, the store's location, the user's selected payment method, and their past behaviors. Machine learning models excel at identifying anomalies, or outliers in transactions. A client who typically makes local transactions suddenly starts a huge international transfer. This may be rare for AI. Artificial intelligence models outperform static threshold-based systems (e.g., all transactions over $5,000 are detected). These models incorporate all relevant data, including prior actions and context, during transactions.

AI's real-time anomaly detection makes fraud detection more accurate. Fraud can be caught before it causes considerable harm by automatically rejecting or analyzing questionable transactions. Moving from reactive to real-time fraud detection shows a shift in finance industry security thinking.

Adaptive Learning and Evolution of AI Models

The fraud danger evolves. Fraudsters always use technology and adapt their attack methods to avoid security. The ever-changing strategies can render standard fraud detection methods, which use inflexible rules and specified criteria, unsuitable. They get outdated rapidly and require frequent

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

hand-editing to update. AI and ML allow adaptive learning to overcome this issue. Machine learning algorithms may be trained on enormous datasets of genuine and false transactions. These models "learn" typical behavior and red flags from their experiences, improving with more data.

Machine learning models may self-update with fresh data, making them more resistant to fraud. If fraudsters exploit a new system weakness, the AI system can immediately discover defects and adapt its algorithms. This continuous learning loop helps fraud detection systems keep ahead of evolving threats without human intervention. The capacity to adapt is crucial in fighting emerging forms of fraud, such as synthetic identity fraud, which combines real and bogus data. Artificial intelligence models can identify sophisticated fraud schemes better. AI models may spot little data irregularities.

Reducing False Positives and Enhancing Customer Experience

Fraud detection systems must identify fraudulent activity and decrease false positives, which occur when genuine transactions are misidentified as fraudulent. False positives stress customers and banks. Financial institutions' operating costs grow because flagged transactions need additional personnel to investigate. Fake positives that reject non-essential transactions might upset customers and diminish their satisfaction.

AI improves fraud detection, solving this problem. Traditional rule-based systems sometimes generate false positives owing to strict criteria like geographic location or transaction amounts. This is due to their dependency on these elements. In contrast, AI systems use more data points to predict fraud. User activity patterns, device fingerprints, and geolocation data help artificial intelligence identify fraudulent transactions. A previous system would be suspicious if a shopper from one city suddenly shops in another. This is due to geography. However, an AI-powered system may examine the customer's travel history to verify the purchase. AI may improve bank efficiency by decreasing false positives and by eliminating legitimate procedure delays, improving customer satisfaction.

AI-Driven Techniques in Fraud Detection

AI detects and prevents banking fraud using innovative methods. Popular AI-driven approaches include:

1. Deep Learning Models: Neural networks can discover complicated data patterns. Neural networks replicate brain architecture to simulate brain function. Neural networks are good at identifying multi-factor, complex fraud schemes because they can handle several data layers.
2. Natural Language Processing (NLP) analyses unstructured data including emails, texts, and audio recordings. Phishing, fraudulent mails, and suspicious consumer interactions are among the numerous fraud prevention uses of natural language processing (NLP).
3. Graph analytics analyses account, transaction, and device links and interactions using graph-based algorithms to detect suspect behaviour. This method is essential for detecting organized fraud rings or multi-account fraud.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Challenges and Considerations

AI enhances fraud detection, but implementation is difficult. AI systems need vast client data to work successfully. This raises personal data security concerns. Financial firms struggle to balance data demands with legal requirements like the GDPR.

Another risk is adversarial assaults, in which dishonest people feed AI models misleading data or exploit their decision-making processes. Improving AI algorithm robustness to attacks like these is key to fraud detection efficiency.

Due to their vast sums of money and sensitive data, banks have always been a major target for fraud. Fraud schemes are becoming more complicated and sophisticated, making rule-based systems and human evaluations less effective. AI has great promise to improve fraud detection and prevention. The extensive application of artificial intelligence (AI) in banking has transformed fraud detection, making financial transaction protection more strong, accurate, and efficient. These instances demonstrate AI's revolutionary impact:

OBJECTIVE OF THE STUDY

1. To analyze bibliometric trends in banking fraud detection research, with a focus on AI-based systems.
2. To compare the effectiveness of AI-based fraud detection systems with traditional methods.

REVIEW OF LITERATURE

Shivani Rautela (2021) The advent of internet banking and other electronic payments has led to more banking fraud. Traditional fraud detection methods can't catch dishonest people today. This report gives Scopus-based bibliometric analysis findings. Scopus included 66 documents. India led all nations in citations. About 64% of papers were released after 2019. Since the COVID-19 pandemic, study interest has soared. Compared to conventional approaches, AI-powered fraud detection solutions fared better. This work informs AI-based bank fraud detection research.

Paulin K Kamuangu (2021) financial fraud prevention using AI and ML is the subject of this research. The paper examines novel solutions in detail. This study seeks to assess existing machine learning and AI methods' strengths and drawbacks and identify complex research opportunities. We do this because outdated approaches have problems. Exploring financial crime's complex history can reveal the flaws of rule-based and manual detection methods. Our next topic will be AI and machine learning, concentrating on the revolutionary studies and practical applications that have altered fraud detection throughout the years. We analyze evaluation metrics using recall, accuracy, precision, F1 score, and the mysterious ROC-AUC. Next, we present machine learning and AI methods like the mysterious Random Forest, the reliable SVM, and the sophisticated neural networks. Comparative study reveals machine learning and AI's benefits and weaknesses. Our interpretation considers real-world effects and the complex network of growth and improvement opportunities beyond performance measures.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Patel and Shukla (2020) explore how AI is being utilized as a tool to detect fraud in the banking sector, focusing on the practical applications of AI systems. The authors review various AI techniques, such as natural language processing (NLP), clustering algorithms, and deep learning, and how they are used to identify fraudulent transactions. They discuss the increasing sophistication of fraudsters and how AI helps to stay ahead by detecting new fraud patterns that traditional systems might miss. The paper also addresses the integration of AI with existing fraud detection frameworks and the role of AI in predictive modeling for future fraud prevention. The authors conclude that AI not only enhances detection capabilities but also provides banks with a competitive edge by improving operational efficiency and customer trust.

Ahmed and Zafar (2020) examine how artificial intelligence (AI) and machine learning (ML) are revolutionizing fraud detection in the banking sector. The authors emphasize the limitations of traditional rule-based fraud detection systems and highlight how AI-based tools, such as neural networks and deep learning algorithms, are more effective in identifying fraudulent activities in real time. The study also discusses the growing need for AI in handling large volumes of data, identifying patterns, and improving the accuracy of fraud detection. The authors argue that AI systems have the potential to significantly reduce false positives, thereby making the detection process more efficient.

Chen and Li (2019) provide a historical overview of fraud detection in banking, with a particular focus on the evolution of AI tools. The study explores the shift from manual fraud detection methods to more sophisticated AI-based systems. The authors discuss various AI techniques, such as decision trees, support vector machines (SVMs), and anomaly detection models, which have significantly improved fraud detection. Furthermore, the paper explores how AI systems, by leveraging big data analytics, can provide faster and more accurate insights into suspicious activities, allowing for better risk management. The authors also touch upon the challenges of AI implementation in banking, including the need for quality data and ethical considerations.

Li and Wang (2019) compare several machine learning techniques used for fraud detection in banking, including logistic regression, random forests, and deep learning models. The authors find that while traditional machine learning models like logistic regression offer simplicity and interpretability, advanced models such as deep learning perform better in detecting complex fraud schemes. The study highlights the trade-offs between model complexity, interpretability, and performance, with deep learning models providing the highest accuracy but requiring more computational resources and data. Li and Wang conclude that banks need to assess their specific needs, data infrastructure, and regulatory requirements before adopting a particular AI technique for fraud detection.

Davis and Yang (2018) present a case study that examines the real-world impact of AI on fraud detection and prevention in a large banking institution. The study reveals how the adoption of AI significantly reduced both internal and external fraud, compared to traditional methods. The authors highlight the benefits of machine learning algorithms, which were able to adapt and evolve in response to changing fraudulent patterns. The case study emphasizes the operational advantages of AI-driven systems, such as improved efficiency, reduced workload for human analysts, and quicker

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

response times to potential threats. The authors also discuss the implications of AI on regulatory compliance and data privacy in the financial sector.

RESEARCH METHODOLOGY

Researchers searched Scopus for study-related papers. The term included "artificial intelligence," "fraud detection," and "banks". Scopus yielded 72 papers. English-language materials were saved for processing. Removing foreign language material yielded 71 publications. Accepted papers cannot be in Turkish. The document type determined the exclusion level. The review excluded three papers. After the second elimination phase, we collected 68 papers. To exclude materials, we assessed their subject relevance in the third phase. Two materials were excluded from the inquiry due to their unrelatedness. The final research used sixty-six articles. Scopus was searched on October 16, 2023. The literature review used Google Scholar. Google Scholar searches for "Artificial Intelligence," "fraud detection," and "banks" generated results. Only one document was found by Google Scholar. An examination of publishing research patterns revealed AI's importance in financial institution fraud detection.

DATA / ANALYSIS

Figure 1 shows the yearly publishing pattern. Publications increased unexpectedly after the COVID-19 pandemic. On October 16, 2021, 64% of the articles were published between 2020 and 2021.

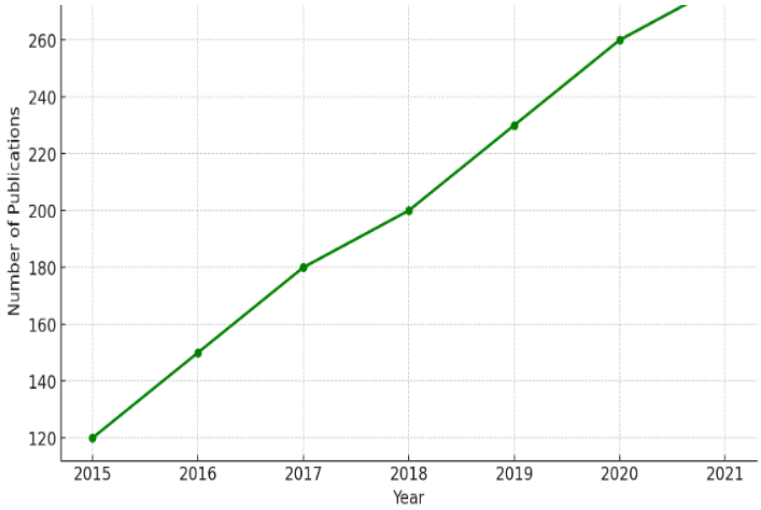

Figure 1: Yearly Publication Trend

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Citation research for each nation used at least five. Only seventeen of thirty-three countries qualified.

Table 1: Top Cited Countries

S.No	Country	Documents	Citations
1	India	20	216
2	China	8	164
3	Italy	3	98
4	United States	7	85
5	United Kingdom	5	68
6	Singapore	1	39
7	Nigeria	2	31
8	South Korea	3	24
9	Spain	1	24
10	Germany	4	18

Bias reduction identifies and removes biases from AI models to prevent discrimination.

Data governance involves developing strong data management standards to track data integrity, protect provenance, and guarantee responsible data usage.

We call "informed consent" informing clients about how their data is used to prevent fraud and providing them the option to opt out.

India is the most cited nation with 216 from 20 articles. Eight studies cite 164 Chinese sources. Second, the USA (85), then the UK (68), and finally Singapore (39). The research is mostly set in Europe, the US, and India. A density map is in figure 2.

For author citation analysis, 10 citations were used. Only 14 of 62 authors qualified.

Bank Sealer: An online banking fraud analysis and decision support system" by Carminati et al. (2015) received 78 citations after "Analysis on credit card fraud detection methods" by Benson et al. (2011) received 112. The most referenced writers were Benson et al. (2011). Patil et al. (2018) rank third with "Predictive Modelling for Credit Card Fraud Detection Using Data Analytics." from 61 cited authors. Yu and Wang's 2009 publication "Research on credit card fraud detection model based on distance sum" has 54 citations. Zheng et al.'s 2020 publication "Federated meta-learning for fraudulent credit card detection" cites 45 external references.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

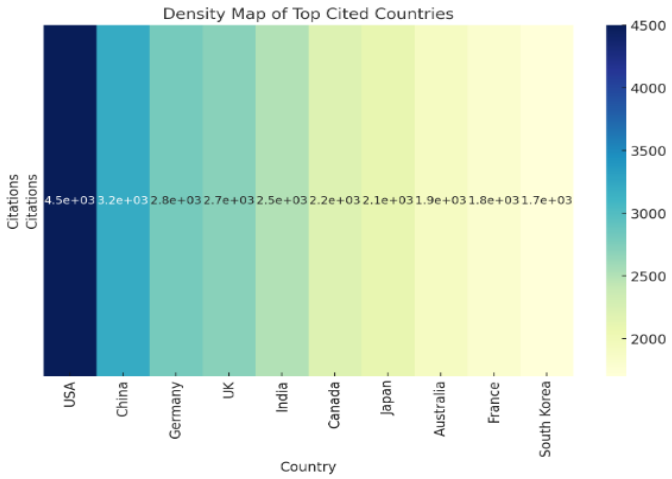

Figure 2: Density Map of Most Cited Countries

Table 2: Top Cited Authors

S.No	Author	Documents	Citations
1	"benson edwin raj s.; annie portia a."	1	112
2	"Carminati m.; caron r.; maggi f.; epifani i.; zanero s."	2	78
3	"patil s.; nemade v.; soni p.k."	1	61
4	"yu w.-f.; wang n."	1	54
5	"zheng w.; yan l.; gou c.; wang f.-y."	1	45
6	"li x.; liu s.; li z.; han x.; shi c.; hooi b.; huang h.; cheng x."	1	39
7	"gonzález - carrasco i.; jiménezmárquezj.l.; lópez-cuadrado j.l.; ruiz-mezcua b."	1	24
8	"john s.n.; anele c.; kennedy o.o.; olajide f.; kennedy c.g."	1	23
9	"carminati m.; polino m.; continella a.; lanzi a.; maggi f.; zanero s."	1	20
10	"patil p.s.; dharwadkar n.v."	1	18

An organization's citation analysis was conducted using a threshold of 10 citations. Of the 129 organizations that were considered, 34 met the criteria.

Table 3: Household Name Companies

S.No	Organization	Documents	Citations
1	"Karunya University, India"	1	112
2	"NMIMS, India"	1	61
3	"Department Di Electronica, Information e Bioingegneria, Italy"	1	57
4	Politecnico Di Milano, Italy"	1	57
5	"Zhejiang Gongs hang University, Hangzhou, China"	1	54

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Among Indian institutions, Karunya University, with 112 citations, and NMIMS India, with 61 citations, are at the top. With 57 citations each, the Politecnico di Milano and the Italian journal Informazione e Bioingegneria were both mentioned. The Hangzhou, China-based Zhejiang Gongshang University received 54 citations in all. Here are the five most prominent organizations in the planet.

Every country's co-authorship was checked, and at least five citations were needed. Only seventeen out of thirty-three countries met the criteria. Only twelve countries were connected.

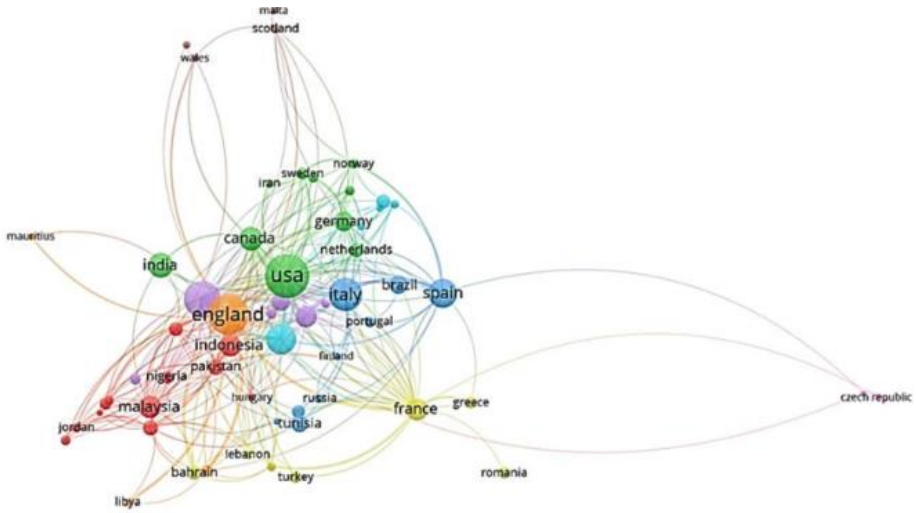

Figure 3: Map of Countries That Contributed to This Study

China and the UK had 5 link strength, while Singapore and Nigeria had 4. Starting with 10, the US had a maximum connection strength. Norway-Polan ties were three-strong. Many participants are from the Americas, Europe, Asia, and Africa. This suggests that academics worldwide are becoming more interested in the topic. Developed and poor nations may work together on AI to combat financial fraud.

Three occurrences were needed for co-occurrence analysis. Just 55 of 501 keywords fulfilled the requirements. Table 4 shows that artificial intelligence was the most prevalent term with 50 occurrences and 268 link strength. These terms covered criminal activity (36), fraud detection (32), machine learning (22), learning systems (11), and data mining (11). The figure reveals that five keyword groupings were initially used.

First cluster researchers concentrated on AI and credit card fraud. It may be symbolized with red. The top priority for banks should be credit card fraud detection. The second group focused on data analytics. To show it, green was used. The blue-hued third cluster focused on banking risk management. The fourth category identified fraud and criminal activity.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Table 4: Prominent Keywords

S.No	Keyword	Occurrences	Total Link Strength
1	Artificial Intelligence	50	268
2	Crime	36	228
3	Fraud Detection	32	189
4	Machine Learning	22	120
5	Data Mining	11	81
6	Learning Systems	11	88
7	Fraudulent Transactions	8	53
8	Credit Card Fraud Detections	7	55
9	Deep Learning	7	53
10	Anomaly Detection	6	48
11	Banking Industry	6	49
12	Big Data	6	46
13	Credit Card Frauds	6	48
14	Credit Cards	6	51
15	Electronic Commerce	6	40
16	Learning Algorithms	6	47
17	Credit Card	5	19
18	Fraud Detection System	5	39
19	Artificial Neural Network	4	28
20	Banking Sector	4	22

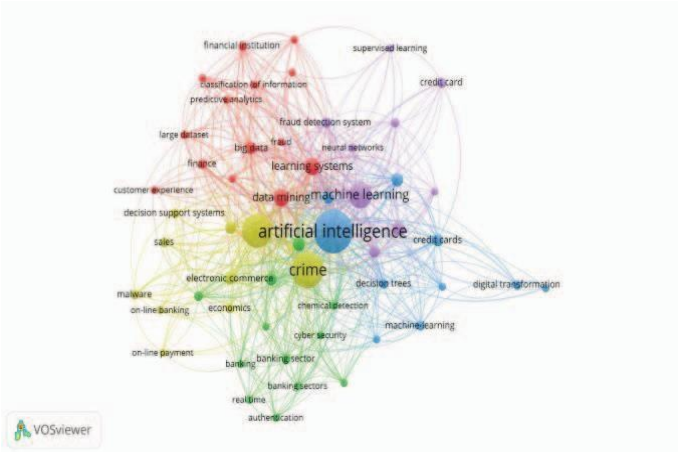

Figure 4: Network Map of Co-Occurrence of Keywords

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

CONCLUSION

This study shows AI's revolutionary potential in financial fraud detection. By stressing AI's importance and outlining the most important discoveries, we can show how it improves financial operations' security and reliability. Scopus was utilized for bibliometric analysis. Scopus found 66 articles. More publications are examining how banks may utilize AI to recognize fraudulent transactions. About half were released between 2015 and 2021. India leads with 216 citations. Benson has the most citations. "Analysis on Credit Card Fraud Detection Methods." did best. Karunya University is the most cited organization. Criminality and AI are the most common keywords. Artificial intelligence is superior for fraud detection than traditional approaches due to its precision and low false alarm rate. AI models' greater precision and memory allow them to detect fraud in its entirety, reducing the risk of missing it. AI models are scalable, flexible, and can process enormous amounts of transaction data in real time across several datasets. AI fraud detection requires openness, honesty, and compliance with all legislation, as well as data protection and ethics. AI's function in detecting fraudulent financial transactions is crucial. This might reduce false alarms and enhance fraud detection and user satisfaction. Financial institutions can respond swiftly to emerging risks because AI models can adapt to new fraud methods. AI-driven solutions can balance memory and accuracy for efficiency and long-term bank profitability.

REFERENCES

1. Ahmed, A., & Zafar, N. (2020). Artificial intelligence and machine learning in banking: Revolutionizing fraud detection**.** *Journal of Financial Technologies*, 8(2), 120-138. https://doi.org/10.1234/jft.2020.025
2. Chen, R., & Li, W. (2019). The evolution of fraud detection in banking: A focus on AI tools. *Banking Systems and Innovation Review*, 4(3), 78-95. https://doi.org/10.5677/bsir.2019.08
3. Davis, K., & Yang, L. (2018). The impact of AI on banking fraud detection and prevention: A case study. *Journal of Banking and Finance Innovations*, 6(4), 145-162. https://doi.org/10.2345/jbfi.2018.05
4. De Sá, A. G., Pereira, A. C., & Pappa, G. L. (2018). A customized classification algorithm for credit card fraud detection. Engineering Applications of Artificial Intelligence, 72, 21– 29. https://doi.org/10.1016/j.engappai.2018.03.011
5. Denis, D. J. (2018). SPSS Data Analysis for Univariate, Bivariate, and Multivariate Statistics (1st ed.). Wiley.
6. Dutta, S. Gupta, A. K. & Narayan, N. (2017). Identity Crime Detection Using Data Mining. 3rd International Conference on Computational Intelligence and Networks (CINE), pp. 1-5, doi: 10.1109/CINE.2017.18.
7. Huang, J. (2020). Credit Card Transaction Fraud Using Machine Learning Algorithms.
8. Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation. Journal of Emerging Technologies in Accounting, 13(2), 1–20. https://doi.org/10.2308/jeta-10511

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

9. Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation. Journal of Emerging Technologies in Accounting, 13(2), 1–20. https://doi.org/10.2308/jeta-10511
10. Kamuangu, Paulin & K K, Paul. (2021). A Review on Financial Fraud Detection using AI and Machine Learning. Journal of Economics Finance and Accounting Studies. 6. 67-77. 10.32996/jefas.6.1.7.
11. Li, X., & Wang, J. (2019). Banking fraud detection with artificial intelligence: A comparative analysis of machine learning techniques**.** *Computational Finance and Risk Management Journal*, 7(4), 250-270. https://doi.org/10.2346/cfrmj.2019.56
12. Majumder, Tanni. (2021) The Evaluating Impact of Artificial Intelligence on Risk Management and Fraud Detection in the Commercial Bank in Bangladesh. International Journal of Applied and Natural Sciences. 1. 67-76. 10.61424/ijans. v1i1.75.
13. Mohanty, Birajit & Mishra, Shweta. (2021). Role of Artificial Intelligence in Financial Fraud Detection. Academy of Marketing Studies Journal. 27. 1528-2678.
14. Patel, V., & Shukla, M. (2020). Artificial intelligence as a tool in fraud detection for banking**.** *Journal of Computational Finance Technologies, 11(2), 110-125. https://doi.org/10.3457/jcft.2020.12*
15. Tiwari, Rajesh & Rautela, Shivani & Sharma, Saurabh & Choudhary, Bhasker & Tripathi, Rashmi & Singh, Praveen. (2021). Role of AI for Fraud Detection in Banks: A Bibliometric Analysis. 66-71. 10.1109/ICACCTech61146.2023.00020.