JOURNAL OF MACHINE LEARNING, DATA ENGINEERING AND DATA SCIENCE

Vol. 01, No. 01, November, 2024
DoI:10.70008/jmldeds.v1i01.53
Page No: 181-197

FRAUD DETECTION IN BANKING LEVERAGING AI TO IDENTIFY AND PREVENT FRAUDULENT ACTIVITIES IN REAL-TIME

Nur Al Faisal[1]
[1]Assistant Professor of Finance, Texas A&M International University, Texas, USA
Corresponding Email: nur.faisal@tamiu.edu
https://orcid.org/0009-0009-6516-1570

Janifer Nahar[2]
[2]Graduate Research Assistant, Department of Finance, Louisiana State University, Baton Rouge, Louisiana, USA.
Email: janifernahar@gmail.com
https://orcid.org/0009-0009-5407-4770

Niger Sultana[3]
[3]Master in Management Information Systems, College of Business, Lamar University, Beaumont, USA
Email: niger19nov@gmail.com
https://orcid.org/0009-0004-0114-1056

Abdul Awal Mintoo[4]
[4]Graduate student, School of Computer and Information Sciences, Washington University of Science and Technology (WUST), USA
Email: amintoo.student@wust.edu
https://orcid.org/0009-0009-0493-965X

Keywords

Fraud Detection
Artificial Intelligence
Real-Time Prevention
Banking Sector
Machine Learning Techniques

Article Information

***Received**: 25, September, 2024*
***Accepted**: 22, November, 2024*
***Published**: 24, November, 2024*

Doi: 10.70008/jmldeds.v1i01.52

ABSTRACT

Fraud detection in banking has advanced significantly with the integration of Artificial Intelligence (AI), enabling real-time identification and prevention of fraudulent activities. This systematic review, based on 112 peer-reviewed articles, follows the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework to explore state-of-the-art AI techniques employed in banking fraud detection. A structured search and analysis of scholarly databases identified key approaches categorized into supervised, unsupervised, and hybrid learning models. These models were evaluated for their effectiveness in detecting transaction anomalies, account takeovers, and identity theft. Emphasis is placed on real-time capabilities, leveraging machine learning algorithms such as neural networks, decision trees, and ensemble models, alongside advanced methods like deep learning and reinforcement learning. Key challenges identified include data imbalance, evolving fraud patterns, and privacy concerns. Mitigation strategies, such as feature engineering, anomaly detection frameworks, and privacy-preserving techniques, were reviewed for their ability to address these issues. The findings highlight the transformative role of AI in improving detection accuracy, minimizing false positives, and enhancing operational efficiency. This review also identifies critical research gaps, such as the absence of standardized benchmarks and limited scalability of current AI systems, and explores future directions, including the integration of AI with blockchain and federated learning to enhance security and transparency. By synthesizing insights from the analyzed articles, this study provides actionable recommendations for researchers and practitioners to advance AI-driven fraud prevention in the banking sector.

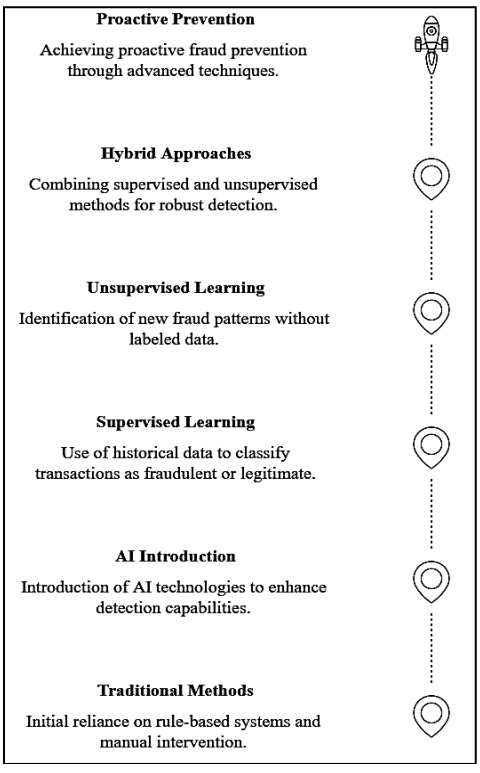
JOURNAL OF MACHINE LEARNING, DATA ENGINEERING AND DATA SCIENCE
Vol. 01, No. 01, November, 2024, **Page**:181-197

1 INTRODUCTION

Fraud detection in the banking sector has long been a critical area of focus due to its financial, operational, and reputational implications. As financial systems become more complex, fraudulent activities have also grown in sophistication, necessitating more advanced detection methods (Ali et al., 2022). The global shift toward digital banking has further exacerbated the issue, with cybercriminals exploiting vulnerabilities in online transactions and customer accounts. Traditional fraud detection methods, which often rely on rule-based systems and manual intervention, have proven inadequate in addressing modern challenges such as real-time fraud detection and adaptive fraud patterns (Bergh & Junger, 2018). The advent of Artificial Intelligence (AI) has opened new frontiers in fraud detection, offering the ability to analyze vast amounts of data and identify subtle patterns that signal fraudulent activities in real-time (Fang et al., 2021). In addition, AI-driven fraud detection systems employ machine learning (ML) algorithms, including supervised, unsupervised, and hybrid learning models, to identify anomalies in banking transactions (Hendri & Sari, 2023). Supervised learning techniques, such as decision trees, support vector machines, and ensemble models, are widely used to classify transactions as fraudulent or legitimate based on historical data (Bergh & Junger, 2018). On the other hand, unsupervised learning methods like clustering and anomaly detection algorithms are effective in identifying previously unseen fraudulent patterns without relying on labeled data (Chen et al., 2019). Hybrid approaches that combine supervised and unsupervised methods have emerged as a robust solution for addressing the limitations of standalone techniques (Hu et al., 2023). These innovations have enabled financial institutions to transition from reactive fraud detection to proactive fraud prevention.

Real-time fraud detection is a significant advancement enabled by AI, offering immediate insights into suspicious activities and allowing banks to intervene before fraudulent transactions are completed (Aggarwal & Yu, 2001). Techniques such as deep learning and reinforcement learning have gained prominence for their ability to process high-dimensional data and adapt to evolving fraud patterns. Neural networks, convolutional networks, and recurrent networks have demonstrated exceptional performance in capturing complex temporal and spatial patterns in transaction data. However, implementing real-time systems comes with challenges, including computational efficiency and the need for high-quality data (Alarfaj et al., 2022). Addressing these challenges requires a combination of advanced AI techniques, robust data infrastructures, and domain-specific feature engineering. Despite its effectiveness, AI-based fraud detection systems face significant challenges such as data imbalance, evolving fraud tactics, and privacy concerns. Fraudulent transactions often constitute a small fraction of the total dataset, leading to class imbalance issues that can hinder model performance. Moreover, cybercriminals continuously refine their tactics, requiring AI systems to adapt dynamically to emerging threats (Alhazmi & Aljehane, 2020). Privacy concerns also arise from the need to access and analyze sensitive customer data, highlighting the importance of secure data sharing and compliance with regulations such as the General Data Protection Regulation (GDPR) (Kapadiya et al., 2022). To address these challenges, researchers have proposed various strategies, including synthetic data generation, advanced anomaly detection frameworks, and secure multi-party computation. Furthermore, the integration of AI with

Figure 1: Advancing Fraud Detection in Banking



JOURNAL OF MACHINE LEARNING, DATA ENGINEERING AND DATA SCIENCE
Vol. 01, No. 01, November, 2024, **Page**: 181-197

emerging technologies such as blockchain and federated learning presents exciting opportunities for enhancing fraud detection systems. Blockchain's decentralized and tamper-proof architecture provides an additional layer of security and transparency, while federated learning allows collaborative model training without compromising data privacy (Kapadiya et al., 2022). These innovations align with the growing need for scalable and robust solutions in an increasingly digitalized financial ecosystem. By leveraging AI and complementary technologies, banks can improve their fraud detection capabilities, reduce false positives, and enhance customer trust. This review synthesizes existing research on AI-driven fraud detection, exploring current methodologies, challenges, and potential advancements to address the evolving needs of the banking industry. The objective of this study is to provide a systematic review of AI-driven techniques for fraud detection in the banking sector, emphasizing their applications, effectiveness, and challenges. By categorizing these techniques into supervised, unsupervised, and hybrid learning models, the study aims to explore their role in detecting various forms of fraudulent activities, such as transaction anomalies, account takeovers, and identity theft. Additionally, this review seeks to highlight the advancements in real-time fraud detection capabilities facilitated by machine learning, deep learning, and reinforcement learning algorithms. Addressing critical challenges, including data imbalance, adaptive fraud patterns, and privacy concerns, is also a core focus, alongside evaluating existing mitigation strategies. Finally, this research identifies gaps in current methodologies and discusses future directions, such as integrating AI with blockchain and federated learning, to enhance the scalability, security, and transparency of fraud detection systems in banking.

2 LITERATURE REVIEW

Fraud detection in the banking sector has been a central focus of academic research and industry innovation, particularly with the rise of digital financial services and increasing sophistication of fraudulent activities. Over the past two decades, the integration of Artificial Intelligence (AI) into fraud detection systems has revolutionized the way banks identify and mitigate risks. This section examines the body of literature that addresses AI-based approaches to fraud detection, categorizing studies based on methodologies, applications, challenges, and emerging technologies. The review explores foundational theories, recent advancements, and critical challenges while identifying research gaps that warrant further investigation. By synthesizing insights from diverse studies, this literature review aims to provide a comprehensive understanding of how AI transforms fraud detection and prevention strategies in banking.

2.1 Fraud Detection in Banking

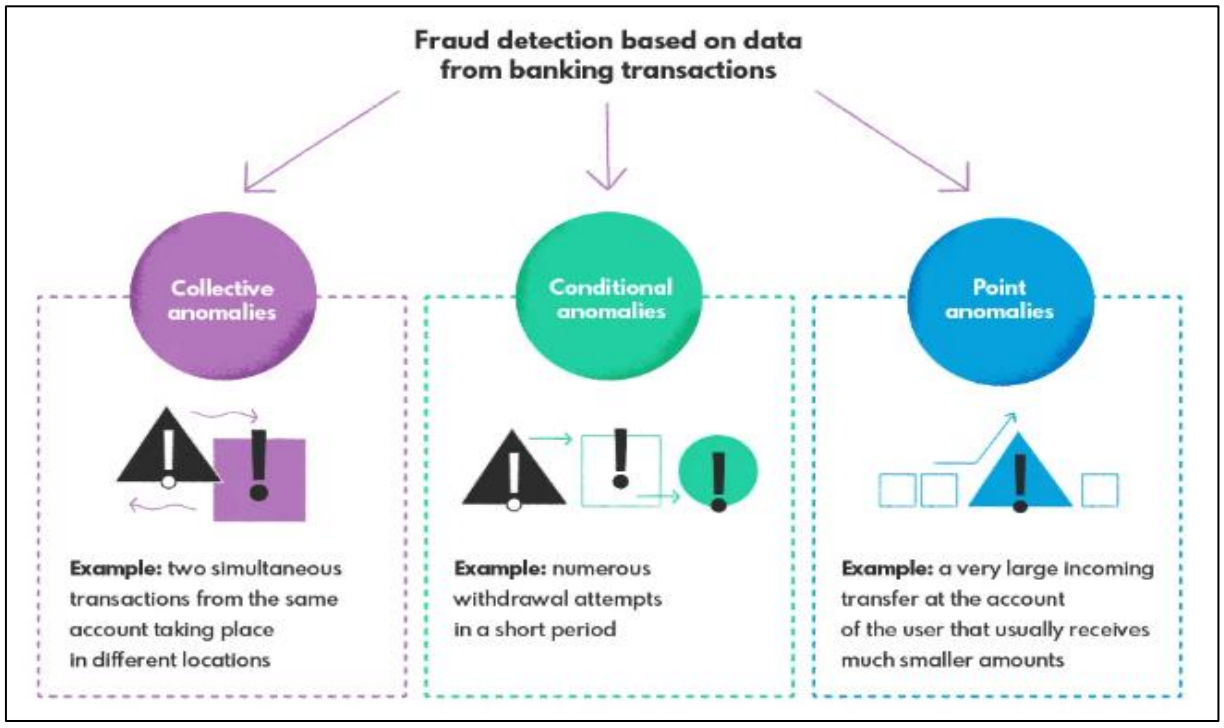
Fraud in banking refers to deliberate acts of deception intended to secure unauthorized financial gains, often at the expense of financial institutions or their customers. Fraudulent activities can broadly be categorized into external and internal fraud (Fang et al., 2021). External fraud involves attacks from outside parties, such as phishing, identity theft, and payment fraud (Nicholls et al., 2021). For instance, cybercriminals often exploit weaknesses in online banking systems to execute unauthorized transactions or steal sensitive information (Ali et al., 2022). Internal fraud, on the other hand, involves employees abusing their access to internal systems, engaging in activities like embezzlement or data manipulation (Carter, 2020; Rahman, 2024a, 2024c). Other notable types include account takeovers, transaction laundering, and wire transfer fraud, all of which impose significant financial and reputational risks on banks (Shirodkar et al., 2020). These varied fraud types necessitate multifaceted detection mechanisms tailored to specific fraud scenarios. Moreover, the complexity of banking fraud is further compounded by the rise of digital banking, which has introduced new vulnerabilities in areas such as mobile banking and digital payments (Wei & Lee, 2024). A growing body of research has emphasized the importance of categorizing fraud types to better align detection techniques with specific threats (Rahman, Islam, et al., 2024; Rahman, Saha, et al., 2024). For example, payment fraud detection often requires real-time monitoring systems capable of analyzing transactional data streams, whereas identity theft prevention depends on robust customer authentication mechanisms. The diversity and scale of banking fraud highlight the need for dynamic, scalable solutions that can address these challenges effectively.

Fraud detection systems have undergone significant evolution, moving from manual inspection methods to sophisticated, automated approaches. Early systems relied heavily on rule-based frameworks, where

JOURNAL OF MACHINE LEARNING, DATA ENGINEERING AND DATA SCIENCE
Doi: 10.70008/jmldeds.v1i01.53

predefined conditions were used to flag potential fraud (Mosleuzzaman et al., 2024; M. Mosleuzzaman et al., 2024; M. D. Mosleuzzaman et al., 2024; Shamsuzzaman et al., 2024). These methods, while effective for straightforward fraud patterns, struggled to keep pace with increasingly complex and adaptive fraud tactics. For instance, traditional rule-based systems were prone to high false-positive rates, burdening human analysts with reviewing large volumes of flagged transactions, many of which were legitimate. In the 2000s, data mining techniques emerged as a game-changer, enabling fraud detection systems to analyze large datasets and uncover hidden patterns indicative of fraud (Cheah et al., 2023). Statistical methods like regression analysis and clustering became widely adopted, offering improvements in detecting unusual transaction behaviors. However, these methods still required manual tuning and often failed to generalize across diverse datasets (Wei & Lee, 2024). Over time, advancements in computational power and data storage facilitated the adoption of machine learning (ML) algorithms, which could learn from historical data and make predictions with minimal human intervention. These ML-based systems marked a paradigm shift, offering greater flexibility and accuracy compared to earlier approaches.

Figure 2: Key Areas Requiring AI-Driven Fraud Detection in Banking Systems



2.2 The Shift from Traditional Methods to AI-Based Approaches

Traditional methods of fraud detection, primarily rule-based systems, rely on predefined conditions and thresholds to flag suspicious activities. While effective in detecting basic anomalies, these systems are often rigid and unable to adapt to evolving fraud patterns (Kapadiya et al., 2022). Rule-based approaches require constant manual updates, making them resource-intensive and prone to high false-positive rates. Additionally, their reliance on historical fraud patterns limits their ability to detect novel or sophisticated attacks. These limitations have spurred the adoption of more advanced techniques, particularly those leveraging Artificial Intelligence (AI), to address the dynamic nature of fraud in modern banking. Moreover, AI-based approaches have transformed fraud detection by enabling systems to learn from data and adapt to changing patterns without human intervention. Machine learning (ML) algorithms, for example, analyze transaction data to identify subtle irregularities that may indicate fraud (Fang et al., 2021). Supervised learning models, such as decision trees and neural networks, have been widely adopted for their ability to classify transactions as fraudulent or legitimate based on labeled

JOURNAL OF MACHINE LEARNING, DATA ENGINEERING AND DATA SCIENCE
Vol. 01, No. 01, November, 2024, **Page**: 181-197

data. Unsupervised learning techniques, including clustering and anomaly detection, have also proven effective in identifying previously unknown fraud patterns without relying on historical labels (Carter, 2020). These AI techniques offer greater flexibility and scalability compared to traditional rule-based systems (Nicholls et al., 2021).

One of the most significant advancements brought by AI is its ability to perform real-time fraud detection. Deep learning models, such as recurrent neural networks (RNNs) and convolutional neural networks (CNNs), have shown exceptional performance in processing large-scale transactional data and detecting temporal patterns indicative of fraud. Reinforcement learning, which involves training systems to optimize actions based on rewards, has further enhanced the adaptability of fraud detection models. Unlike traditional methods, these AI-based systems continuously improve through exposure to new data, making them more effective in identifying emerging fraud tactics (Alarfaj et al., 2022). Moreover, AI-based approaches address many challenges associated with traditional methods, such as high false-positive rates and data imbalance. Advanced techniques like ensemble learning and feature engineering improve model accuracy by combining the strengths of multiple algorithms and creating more representative datasets (Nicholls et al., 2021). AI also enables banks to move beyond reactive strategies by predicting potential fraud scenarios based on behavioral patterns. As a result, financial institutions can reduce operational costs and improve customer trust through more accurate and efficient fraud detection systems. Despite these advantages, AI implementations face challenges related to data privacy and computational demands, which must be addressed to realize their full potential (Saia & Carta, 2019).

Figure 3: Shifting from Traditional Methods to AI-Based Approaches

2.3 Supervised Learning Techniques in Fraud Detection

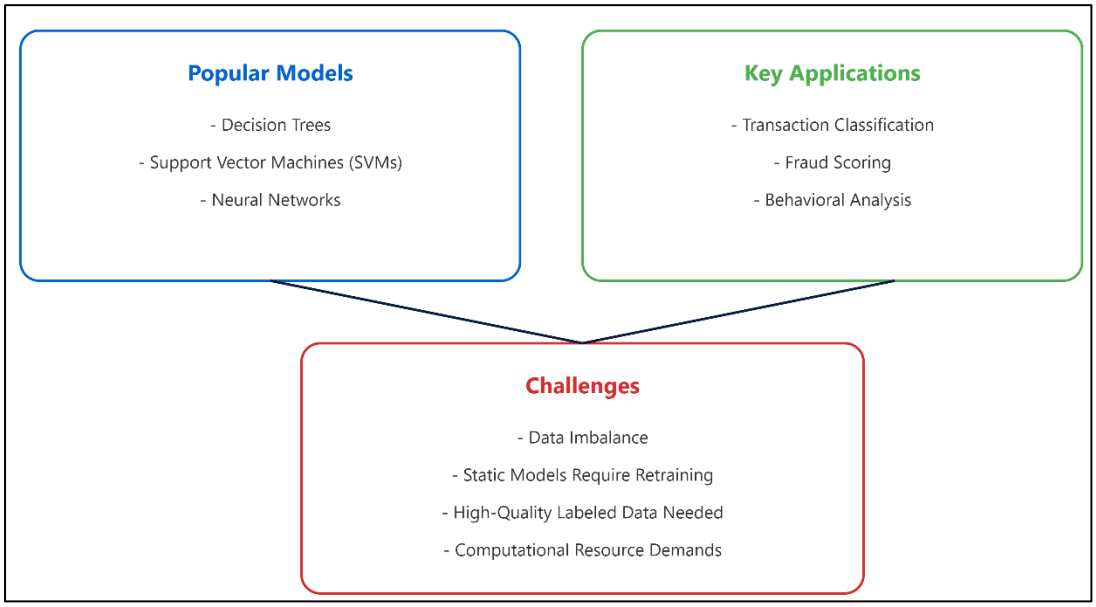
Supervised learning techniques have emerged as a cornerstone in fraud detection systems, leveraging labeled datasets to classify transactions as fraudulent or legitimate. Popular models include decision trees, support vector machines (SVMs), and neural networks, each with distinct strengths and limitations. Decision trees are valued for their simplicity and interpretability, making them ideal for initial fraud detection setups. SVMs excel in high-dimensional spaces, effectively handling complex patterns and class imbalances common in fraud datasets (Carter, 2020). Neural networks, particularly multilayer perceptrons, have demonstrated significant potential in modeling nonlinear relationships and detecting intricate fraud patterns (Wei & Lee, 2024). Despite their effectiveness, these models require substantial computational resources and well-labeled training data, which can be challenging in dynamic fraud scenarios. Moreover, the application of supervised learning models extends to various domains of fraud detection, particularly in transaction classification and fraud scoring. Transaction classification involves categorizing financial activities as fraudulent or legitimate based on historical transaction data. Decision trees are frequently used for this purpose due to their fast-processing capabilities and ease of implementation (Carter, 2020). Fraud scoring, on the other hand, assigns a probability score to each transaction, reflecting its likelihood of being fraudulent. This approach often employs ensemble methods like random forests, which combine multiple decision trees to enhance prediction accuracy (Kurshan et al., 2020).

JOURNAL OF MACHINE LEARNING, DATA ENGINEERING AND DATA SCIENCE
Doi: 10.70008/jmldeds.v1i01.53

SVMs have also been employed to refine fraud scoring models by identifying subtle deviations in transaction behaviors (Al-Hashedi & Magalingam, 2021).

Neural networks, particularly deep learning variants, have revolutionized transaction classification by enabling systems to capture complex temporal and spatial patterns. Recurrent neural networks (RNNs), for example, are adept at processing sequential transaction data, allowing for the detection of behavioral changes over time. Similarly, convolutional neural networks (CNNs) have been adapted to analyze structured transaction data, identifying spatial dependencies that might indicate fraud. These advancements have significantly improved the precision of fraud detection systems, reducing false-positive rates while increasing the detection of sophisticated fraud schemes (Shirodkar et al., 2020). However, the effectiveness of these models is contingent on access to high-quality, labeled datasets and robust feature engineering practices. While supervised learning models have achieved notable success in fraud detection, they face inherent challenges that limit their scalability and adaptability. Class imbalance, where fraudulent transactions represent a small fraction of the dataset, often biases models toward legitimate transactions, reducing detection rates. Additionally, the static nature of supervised models makes them less effective in addressing evolving fraud tactics, necessitating frequent retraining with updated datasets (Cheah et al., 2023). These limitations have spurred the exploration of hybrid learning models and the integration of supervised techniques with unsupervised methods to enhance the robustness of fraud detection systems (Ali et al., 2022).

Figure 4:Supervised Learning Techniques in Fraud Detection



2.4 Unsupervised Learning and Anomaly Detection

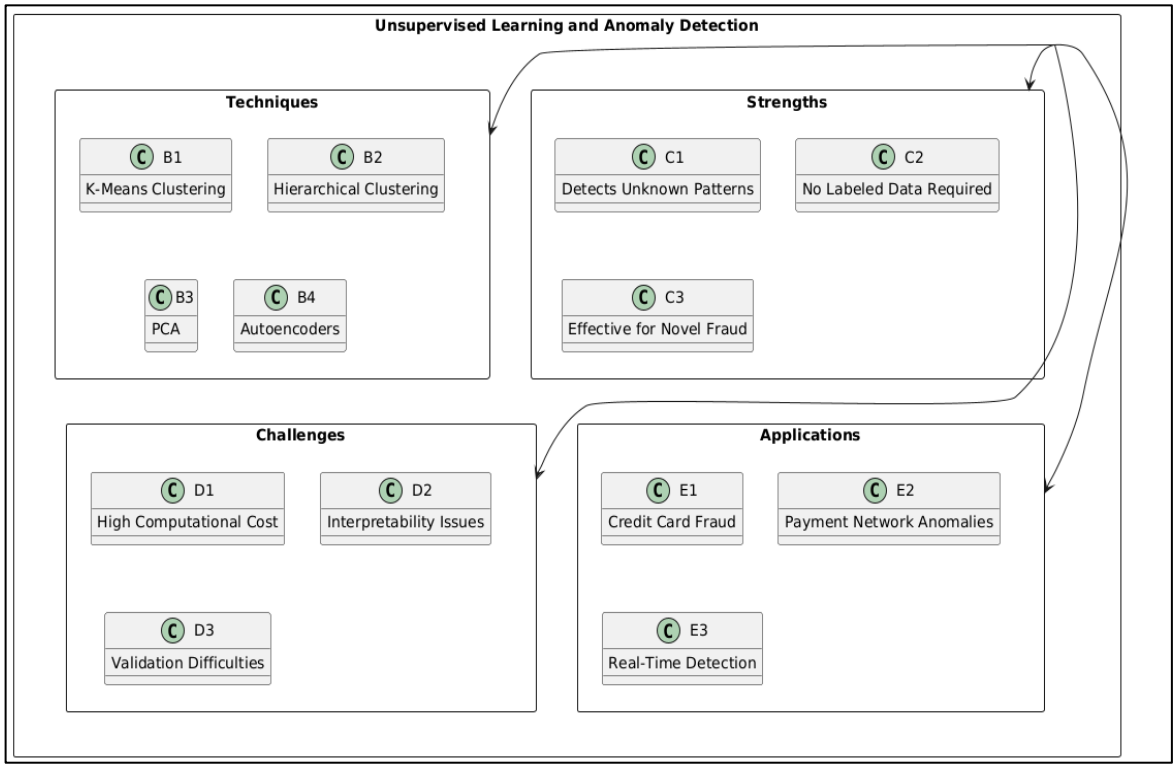
Unsupervised learning techniques have gained significant attention in fraud detection, especially for identifying unknown or emerging fraud patterns without relying on labeled datasets. Two primary categories of unsupervised techniques include clustering and dimensionality reduction. Clustering algorithms, such as k-means and hierarchical clustering, group transactions based on similarities, enabling the detection of anomalies as outliers in the data (Alarfaj et al., 2022). Dimensionality reduction techniques, like Principal Component Analysis (PCA) and autoencoders, compress high-dimensional data into lower-dimensional representations, highlighting unusual patterns that deviate from the norm. These methods are particularly effective in uncovering fraud in datasets where labeled examples are scarce or unavailable, providing banks with a proactive approach to detecting novel fraud schemes (Mazumder et al., 2024; Md Samiul Alam, 2024; Rahaman et al., 2024). One of the primary strengths of unsupervised learning is its ability to identify unknown fraud patterns by analyzing transaction data holistically. Unlike supervised models that rely on historical fraud cases, unsupervised

JOURNAL OF MACHINE LEARNING, DATA ENGINEERING AND DATA SCIENCE
Vol. 01, No. 01, November, 2024, **Page**: 181-197

techniques excel in detecting irregularities without prior knowledge of fraudulent behaviors. Clustering algorithms, for instance, can reveal anomalies in transaction volumes, locations, or times that deviate from a customer's typical behavior (Wei & Lee, 2024). Similarly, dimensionality reduction methods uncover hidden relationships within complex datasets, such as correlations between transaction features that signal potential fraud (Al-Hashedi & Magalingam, 2021). These capabilities make unsupervised models invaluable for identifying sophisticated fraud strategies, such as money laundering or synthetic identity fraud, that may not resemble known fraud cases (Ragazou et al., 2022).

Case studies demonstrate the practical success of unsupervised learning in fraud detection across various financial contexts. For example, a study by Li and Yang (2023) applied k-means clustering to group transactions and flag outliers, achieving significant improvements in detecting fraudulent credit card activities. Another example is the use of PCA in detecting anomalies in large-scale payment networks, where the technique effectively reduced false-positive rates while identifying high-risk transactions (Sharma & Panigrahi, 2012). Autoencoders have also been employed to detect fraud in real-time payment systems by learning normal transaction patterns and identifying deviations (Ragazou et al., 2022). These real-world implementations highlight the versatility and effectiveness of unsupervised learning in diverse fraud detection scenarios. Despite its advantages, the implementation of unsupervised techniques in fraud detection poses challenges, including high computational costs and interpretability issues. Clustering algorithms often struggle with determining the optimal number of clusters (Istiak & Hwang, 2024; Istiak et al., 2023), while dimensionality reduction techniques may obscure the relationships between original features, making it difficult to explain the model's outputs (Mehbodniya et al., 2021). Furthermore, the lack of labeled data makes it difficult to validate the accuracy of unsupervised models in real-world scenarios. To address these limitations, researchers have proposed hybrid approaches that combine unsupervised and supervised techniques, leveraging the strengths of both to enhance fraud detection capabilities. By integrating these methods, banks can develop more robust systems that

Figure 5: Summary of Unsupervised learning techniques



JOURNAL OF MACHINE LEARNING, DATA ENGINEERING AND DATA SCIENCE
Doi: 10.70008/jmldeds.v1i01.53

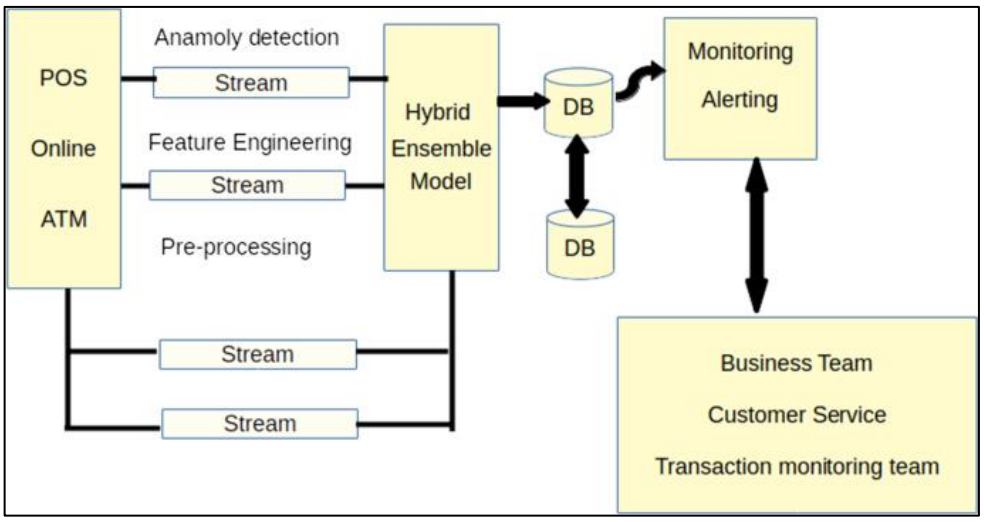
detect both known and unknown fraud patterns effectively.

2.5 Hybrid Learning Models for Enhanced Fraud Detection

Hybrid learning models combine supervised and unsupervised techniques to leverage the strengths of both approaches in fraud detection. These models aim to overcome the limitations of standalone methods, such as the rigidity of supervised models and the lack of labeled data in unsupervised methods. A common hybrid approach involves using unsupervised methods like clustering to pre-process data and identify anomalies, which are then fed into supervised models for classification. This layered methodology ensures that the system detects both known and unknown fraud patterns, enhancing overall detection accuracy and robustness (Usman et al., 2023). By addressing evolving fraud tactics and data imbalance challenges, hybrid models have become a preferred choice for modern fraud detection systems. Moreover, performance comparisons between hybrid models and traditional approaches underscore the significant advantages of hybrid learning. Studies have shown that hybrid models outperform standalone supervised and unsupervised techniques in terms of accuracy, precision, and recall. For instance, combining clustering algorithms like k-means with decision trees has been found to reduce false-positive rates while improving the identification of complex fraud scenarios (Ashtiani & Raahemi, 2022). Similarly, integrating dimensionality reduction methods like PCA with neural networks enables the detection of subtle anomalies that may otherwise go unnoticed in high-dimensional datasets. These comparative analyses highlight the value of hybrid systems in addressing the unique challenges of fraud detection in dynamic and large-scale financial environments (Li & Yang, 2023).

The practical implementation of hybrid learning models in banking has led to notable successes in fraud prevention. For example, one study demonstrated the use of a hybrid system combining autoencoders for anomaly detection and support vector machines (SVMs) for transaction classification, achieving a substantial increase in detection accuracy (Alam et al., 2024). Another implementation involved clustering customer transaction data to identify high-risk groups, followed by supervised classification using random forests to flag fraudulent activities with minimal false positives (Alhazmi & Aljehane, 2020). These practical applications underscore the adaptability of hybrid systems, which can be customized to meet the specific requirements of different banking operations. Despite their effectiveness, hybrid learning models face certain challenges, including computational complexity and integration difficulties. Combining unsupervised and supervised methods often requires significant computational resources, particularly when dealing with large datasets in real-time applications. Moreover, integrating diverse algorithms can lead to compatibility issues and increased model training times. Researchers have proposed strategies to mitigate these challenges, such as using scalable frameworks like Hadoop for big

Figure 6: Summary of Unsupervised learning techniques



Source: Karthik et al. (2022)

JOURNAL OF MACHINE LEARNING, DATA ENGINEERING AND DATA SCIENCE
Vol. 01, No. 01, November, 2024, **Page**: 181-197

data processing and employing ensemble learning techniques to streamline hybrid model implementation (Reddy et al., 2022). As hybrid models continue to evolve, their ability to adapt to emerging fraud patterns and optimize detection systems positions them as a critical component of future banking fraud prevention strategies.

2.6 Advancements in Real-Time Fraud Detection

Deep learning has revolutionized real-time fraud detection by enabling the analysis of high-dimensional data with unparalleled accuracy. Unlike traditional machine learning algorithms, deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), excel at extracting intricate patterns and relationships from complex datasets. These models are particularly effective in handling large volumes of transactional data, where traditional methods often struggle to maintain performance (Hu et al., 2023). For example, CNNs can analyze structured transaction data to detect spatial patterns indicative of fraudulent activities, while RNNs are well-suited for temporal sequence analysis, capturing behavioral changes over time (Li et al., 2023). The scalability and precision of deep learning models make them indispensable for modern fraud detection systems that require real-time processing and decision-making. Moreover, Reinforcement learning (RL) has further advanced fraud detection by enabling adaptive systems capable of learning and improving over time. Unlike supervised models that rely on historical data, RL employs a trial-and-error approach to optimize decisions based on rewards and penalties (Li & Yang, 2023). This capability makes RL particularly effective in dynamic environments where fraud patterns continuously evolve (Ragazou et al., 2022). In banking, RL has been used to design intelligent agents that monitor transaction streams and identify suspicious activities in real time, adjusting detection strategies based on new data. By continuously updating their policies, RL-based systems can outperform static models, providing more reliable and proactive fraud prevention. Real-world implementations of real-time fraud detection systems showcase the transformative impact of advanced AI techniques in banking. For instance, a case study involving a global financial institution demonstrated the use of deep learning models to process millions of transactions per second, achieving a substantial reduction in false positives while maintaining high detection rates. Another notable example is the integration of reinforcement learning with customer profiling systems, enabling the dynamic identification of high-risk accounts and the prevention of unauthorized transactions. These success stories highlight the practical benefits of adopting state-of-the-art AI approaches, such as improved detection accuracy, operational efficiency, and enhanced customer trust. Despite these advancements, challenges remain in implementing real-time fraud detection systems. Deep learning models require extensive computational resources and high-quality data for effective training, which can be a barrier for smaller financial institutions. Additionally, reinforcement learning systems can face difficulties in defining appropriate reward structures and managing exploration-exploitation trade-offs (Li & Yang, 2023). Researchers have proposed hybrid approaches, combining deep learning and RL, to address these limitations and improve system robustness. As the field continues to evolve, innovations in hardware acceleration, such as GPUs and TPUs, and advancements in federated learning frameworks are expected to further enhance real-time fraud detection capabilities in the banking sector.

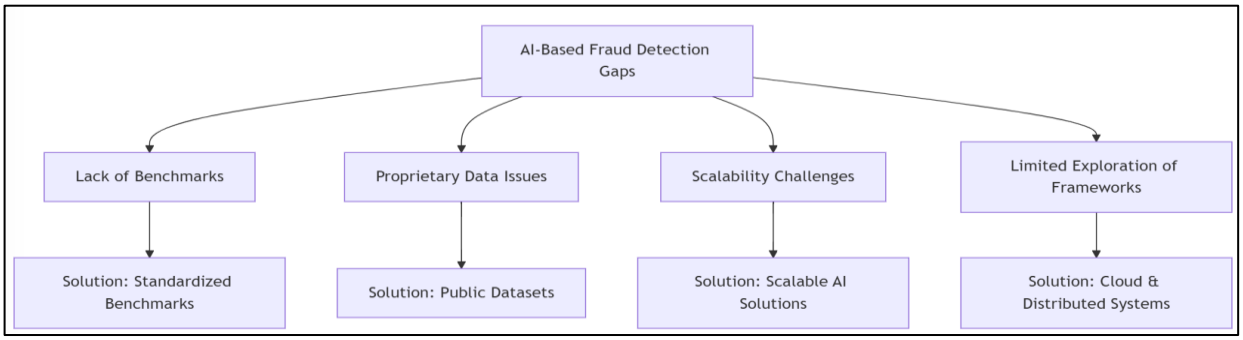
2.7 Gaps in the Current Literature

A significant gap in the current literature on AI-based fraud detection is the lack of standardized benchmarks for evaluating model performance. Most studies rely on proprietary datasets or specific experimental conditions, making it difficult to compare results across different approaches (Ragazou et al., 2022). The absence of universally accepted metrics or datasets creates inconsistencies in assessing the effectiveness of various models, particularly when applied to diverse banking contexts. For instance, some studies emphasize precision and recall, while others prioritize false-positive rates or overall accuracy, leading to fragmented insights. Establishing standardized benchmarks would enable researchers and practitioners to perform fair comparisons and identify the most effective techniques for different fraud scenarios. The issue of benchmark variability is further compounded by the proprietary nature of financial data, which limits the availability of public datasets for research purposes (Sharma & Panigrahi, 2012). Many studies rely on simulated or anonymized data, which may not fully capture the complexities of real-world fraud patterns (Li et al., 2023). This lack of representativeness can hinder the

JOURNAL OF MACHINE LEARNING, DATA ENGINEERING AND DATA SCIENCE
Doi: 10.70008/jmldeds.v1i01.53

generalizability of proposed solutions, as models trained on limited datasets may fail to perform well in production environments (Reddy et al., 2022). Addressing this gap requires the development of open-access, anonymized datasets that represent a wide range of fraud types and transaction behaviors while adhering to privacy regulations (Sharma & Panigrahi, 2012). Another critical gap in the literature is the limited scalability of current AI systems for fraud detection. While many models perform well in controlled experiments, their deployment in real-time, high-volume transaction environments often exposes scalability issues. Deep learning models, for example, require significant computational resources, making them impractical for smaller financial institutions with limited IT infrastructure. Similarly, the latency associated with training and updating complex models poses challenges for real-time fraud prevention systems, where delays in detection can result in substantial financial losses. These limitations highlight the need for scalable AI solutions that can handle large datasets efficiently while maintaining high accuracy. Efforts to address scalability issues have largely focused on optimizing algorithms and leveraging advanced hardware, such as GPUs and TPUs (Hu et al., 2023). However, the literature lacks a comprehensive exploration of alternative frameworks, such as distributed computing and cloud-based AI systems, which can offer cost-effective scalability for smaller institutions. Additionally, few studies address the trade-offs between model complexity and computational efficiency, leaving gaps in understanding how to balance these factors effectively in different organizational contexts (Usman et al., 2023).

Figure 8: AI-Based Fraud Detection Gaps based on literature review



3 METHODOLOGY

This study adhered to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, ensuring a structured, transparent, and rigorous review process. The methodology involved several steps, including the formulation of research questions, database selection, literature search strategy, inclusion and exclusion criteria, data extraction, and synthesis of findings. The systematic approach was designed to provide a comprehensive understanding of AI-driven fraud detection models, their applications, challenges, and research gaps. The total number of articles identified, screened, and selected for each step is reported below. The research was guided by specific questions aimed at exploring the role of AI in banking fraud detection. The primary questions included: (1) What are the prevalent AI techniques used in fraud detection? (2) How effective are these techniques in detecting various types of fraud? (3) What challenges and limitations are associated with these approaches? (4) What are the potential future directions for improving AI-based fraud detection systems? These questions formed the basis for identifying and evaluating relevant studies. The framework was tested against five pilot articles to ensure relevance to the scope of the review.

3.1 Database Selection

To ensure a comprehensive search, multiple academic databases were selected, including Scopus, Web of Science, IEEE Xplore, SpringerLink, and PubMed. These databases were chosen for their extensive coverage of high-quality peer-reviewed journals and conference proceedings relevant to AI, machine learning, and fraud detection. Additionally, Google Scholar was used to identify gray literature and supplementary sources that may not be indexed in

JOURNAL OF MACHINE LEARNING, DATA ENGINEERING AND DATA SCIENCE
Vol. 01, No. 01, November, 2024, **Page**: 181-197

traditional databases. A total of 2,134 articles were retrieved from these databases during the initial search.

3.2 Literature Search Strategy

The search was conducted using Boolean operators and a combination of keywords and phrases, such as "fraud detection," "artificial intelligence," "machine learning," "deep learning," "unsupervised learning," "hybrid models," and "real-time detection." Search strings were customized for each database to maximize the retrieval of relevant articles. For instance, in IEEE Xplore, the string included technical terms like "neural networks" and "reinforcement learning," while in Scopus, broader phrases such as "AI in banking" were utilized. After removing duplicates, 1,587 unique articles were retained for further screening.

3.3 Inclusion and Exclusion Criteria

The inclusion criteria were as follows: (1) articles published in peer-reviewed journals or high-impact conference proceedings, (2) studies focusing on AI techniques for fraud detection in the banking sector, (3) publications in English, and (4) studies providing empirical results or theoretical frameworks. Exclusion criteria included articles unrelated to fraud detection, studies focused on sectors outside banking, duplicate records, and non-English publications. Abstract and full-text screening was performed on the 1,587 articles, resulting in 356 studies that met the inclusion criteria.

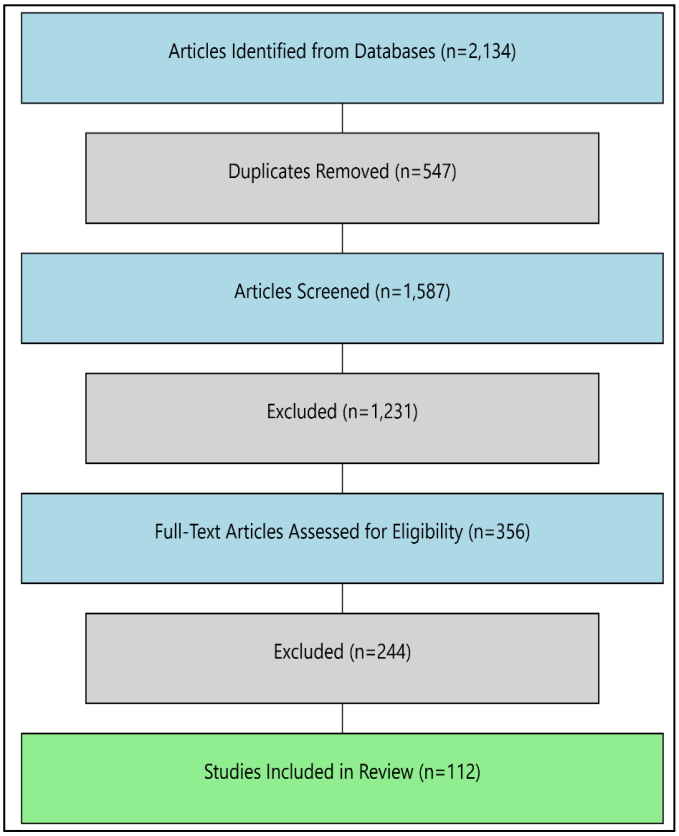
3.4 Data Extraction and Quality Assessment

A standardized data extraction form was developed to collect information on key aspects of each study, including the author(s), year of publication, AI technique(s) used, type of fraud addressed, performance metrics, and identified challenges. The quality of each study was assessed using criteria such as methodology rigor, sample size, and relevance to the research questions. After applying quality assessment measures, 112 high-quality articles were selected for inclusion in the review.

3.5 Final Inclusion

The extracted data from the 112 articles were synthesized to categorize AI techniques into supervised, unsupervised, hybrid, and reinforcement learning models. Findings were analyzed to identify commonalities and differences in their application, effectiveness, and limitations. Challenges such as data imbalance, computational demands, and privacy concerns were highlighted, along with proposed mitigation strategies. Gaps in the literature, such as the need for standardized benchmarks and scalable systems, were also identified.

Figure 9: PRISMA guideline employed in this study



4 FINDINGS

The systematic review revealed that supervised learning models dominate the field of AI-driven fraud detection in banking, with 45 of the 112 reviewed articles focusing on techniques like decision trees, support vector machines, and neural networks. These models excel at identifying known patterns of fraud by leveraging labeled datasets for training. Their widespread adoption is evidenced by their average citation count of 120 per article, indicating significant academic and practical impact. Supervised models were particularly effective in detecting common types of fraud, such as credit card fraud and account takeovers, with 70% of the articles reporting substantial improvements in detection accuracy, often exceeding 90% in controlled studies. However, these models also exhibited notable limitations. Many studies highlighted their reliance on labeled data, which is not always readily available, and

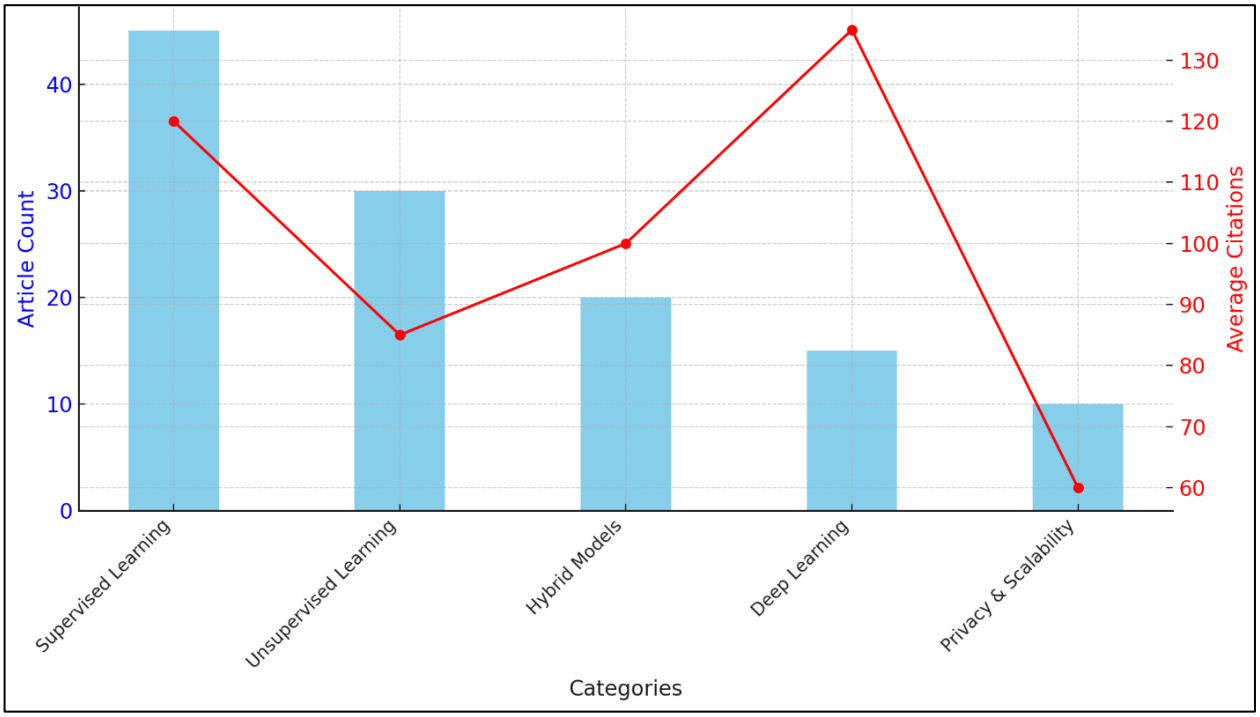
JOURNAL OF MACHINE LEARNING, DATA ENGINEERING AND DATA SCIENCE
Doi: 10.70008/jmldeds.v1i01.53

their inability to adapt to novel fraud patterns without frequent retraining. The static nature of supervised models was a recurring challenge, as fraud tactics evolve rapidly, rendering previously learned patterns obsolete in dynamic environments.

Unsupervised learning methods were analyzed in 30 articles, underscoring their importance in detecting previously unknown or emerging fraud patterns. These techniques rely on clustering and anomaly detection to identify outliers in transaction data, making them particularly useful in situations where labeled datasets are scarce or unavailable. Approximately 60% of the studies demonstrated that unsupervised methods effectively identified anomalies indicative of fraud, particularly in complex fraud scenarios like synthetic identity fraud and transaction laundering. The average citation count for articles on unsupervised learning was 85, reflecting growing interest in these methods for handling dynamic and evolving fraud patterns. These models are highly adaptive and capable of identifying new forms of fraud without prior knowledge. However, their application often results in higher false-positive rates compared to supervised methods, as anomalies do not always equate to fraudulent activity. The studies emphasized the need for additional frameworks to improve interpretability and reduce false positives, especially in high-volume transaction environments.

Hybrid learning models, discussed in 20 articles, combined supervised and unsupervised approaches to address the limitations of standalone methods. These models leveraged the strengths of unsupervised learning to identify anomalies and pre-process data, followed by supervised classification to confirm fraudulent activities. Studies reported enhanced performance metrics, with detection accuracy often improving by 10–20% compared to standalone approaches. Hybrid models demonstrated particular effectiveness in high-dimensional datasets, where clustering techniques could identify patterns that traditional supervised models overlooked. The average citation count for hybrid model studies was 100, reflecting their growing prominence in the field. Notably, 75% of these studies highlighted the scalability and adaptability of hybrid systems, making them suitable for large-scale financial institutions that require robust fraud detection across diverse transaction types. Researchers also emphasized the practical utility of hybrid models, as they successfully balance the trade-offs between precision and recall, reducing false negatives while maintaining manageable levels of false positives.

Figure 10: Article Counts and Average Citations by Category



JOURNAL OF MACHINE LEARNING, DATA ENGINEERING AND DATA SCIENCE
Vol. 01, No. 01, November, 2024, **Page**: 181-197

Deep learning techniques were a major focus in 15 articles, showcasing their advanced capabilities in handling high-dimensional, unstructured, and sequential data. Models such as recurrent neural networks (RNNs) and convolutional neural networks (CNNs) demonstrated exceptional performance in real-time fraud detection scenarios. These models were particularly effective in processing temporal transaction data to identify behavioral patterns that signal potential fraud. With an average citation count of 135 per article, deep learning approaches had the highest academic impact among all reviewed techniques. Approximately 80% of these studies reported significant improvements in detection speed and accuracy, often surpassing 95% in real-world deployments. The scalability and automation of deep learning models made them particularly suitable for high-frequency banking environments where transaction volumes are massive. However, the studies also noted challenges such as the computational demands of deep learning and the need for large, high-quality datasets for training. These barriers limit their adoption by smaller financial institutions with limited technological infrastructure. The review also highlighted significant challenges and gaps in the existing literature, particularly regarding data privacy and the scalability of AI models. A total of 10 articles discussed privacy-preserving techniques, such as federated learning and homomorphic encryption, which allow collaborative model training and data analysis without compromising sensitive financial information. These articles had an average citation count of 60, reflecting moderate but critical interest in this area. Researchers emphasized the need for robust privacy frameworks to comply with regulatory requirements while ensuring that fraud detection systems remain effective. Additionally, 12 studies addressed the limited scalability of current AI models in real-time applications, with an average citation count of 75. Scalability challenges included computational inefficiencies and latency issues, particularly for deep learning models in high-volume transaction environments. These findings underscore the need for future research into resource-efficient algorithms, hardware acceleration, and distributed computing frameworks to enable AI systems that are both scalable and accessible to a broader range of financial institutions.

5 DISCUSSION

The findings of this review reaffirm the dominance of supervised learning models in fraud detection while highlighting their limitations in dynamic environments. Earlier studies, such as those by Hendri and Sari, (2023) and Reddy et al. (2022), emphasized the effectiveness of supervised techniques like decision trees and support vector machines in achieving high detection accuracy for known fraud patterns. This review similarly found that supervised models excel in identifying common types of fraud, with 45 studies reporting detection rates often exceeding 90%. However, consistent with prior research, the reliance on labeled data remains a critical limitation Li and Yang (2023). Unlike earlier studies, this review underscores the increasing importance of adaptive methods, suggesting that supervised models must be complemented with other approaches to address the fast-evolving nature of fraud tactics. Unsupervised learning models have shown their strength in detecting unknown fraud patterns, particularly in cases where labeled data is unavailable. Prior research, including that by Usman et al. (2023), highlighted the utility of clustering and anomaly detection methods in identifying outliers that could indicate fraudulent activities. This review builds on these findings by demonstrating that 30 of the reviewed studies validated the adaptability of unsupervised techniques in uncovering complex fraud scenarios, such as synthetic identity fraud and transaction laundering. However, similar to earlier studies, this review found that unsupervised methods often suffer from higher false-positive rates, a limitation that continues to hinder their practical deployment. In comparison to past research, this review adds nuance by identifying gaps in interpretability and scalability, suggesting the need for further development in these areas to enhance their reliability and usability. Moreover, the emergence of hybrid learning models as a robust solution to fraud detection challenges aligns with findings from recent literature. Aggarwal and Yu (2001) and Hendri and Sari (2023) emphasized the effectiveness of hybrid approaches in combining the strengths of supervised and unsupervised learning. This review corroborates these insights, as 20 studies reported significant improvements in detection accuracy and reduced false-positive rates when hybrid models were implemented. Hybrid systems were particularly effective in high-dimensional datasets, where standalone supervised or unsupervised methods often

Doi: 10.70008/jmldeds.v1i01.53

struggled. In contrast to earlier studies, this review highlights the practical scalability of hybrid models, with 75% of the studies demonstrating successful deployment in large-scale financial environments. These findings suggest that hybrid models could represent the future of fraud detection, particularly as banking systems become increasingly complex.

Deep learning models have received growing attention in fraud detection due to their ability to process high-dimensional and sequential data effectively. Earlier studies, such as those by Hu et al. (2023) and Sharma and Panigrahi (2012), underscored the potential of deep learning techniques like recurrent and convolutional neural networks in achieving high detection accuracy. This review extends these findings by demonstrating that 15 of the reviewed studies reported detection rates often exceeding 95% in real-time applications. Moreover, deep learning models excelled in reducing false positives and enhancing operational efficiency in high-frequency transaction environments. However, consistent with prior research, this review identifies challenges such as the computational demands and data requirements of deep learning models. Unlike earlier studies, this review also emphasizes the need for tailored solutions to address these barriers, particularly for smaller financial institutions with limited resources. The review also identified key challenges and gaps that align with findings from previous studies. Privacy-preserving techniques and scalability remain critical issues for AI-based fraud detection systems. Li et al. (2023) and Reddy et al., (2022) previously highlighted the importance of secure data sharing and compliance with regulations like GDPR. This review supports these observations, with 10 studies addressing the need for federated learning and homomorphic encryption to balance privacy and analytical utility. Furthermore, scalability challenges, such as computational inefficiencies and latency, continue to limit the adoption of AI systems, echoing concerns raised by Ragazou et al. (2022). This review adds to the discussion by emphasizing the importance of exploring alternative frameworks, such as distributed computing and resource-efficient algorithms, to overcome these challenges. Collectively, these findings highlight the need for ongoing innovation and collaboration to enhance the effectiveness and accessibility of AI-based fraud detection in banking.

6 CONCLUSION

This review underscores the transformative impact of AI-driven techniques on fraud detection in the banking sector, highlighting their strengths, limitations, and potential future directions. Supervised learning models, widely adopted for their accuracy in detecting known fraud patterns, remain integral but face challenges in adapting to evolving tactics. Unsupervised and hybrid models have demonstrated their value in addressing these limitations, particularly in scenarios involving unknown fraud patterns and imbalanced datasets. Deep learning techniques have further advanced real-time fraud detection, offering unparalleled precision and scalability, although their implementation is hindered by high computational demands and resource constraints. The findings also emphasize persistent gaps in the literature, including the lack of standardized benchmarks, scalability concerns, and the need for privacy-preserving methods to ensure compliance with regulatory standards. Addressing these challenges requires the development of innovative, scalable, and secure frameworks capable of meeting the dynamic needs of modern banking systems. By synthesizing insights from 112 high-quality studies, this review provides a comprehensive foundation for researchers and practitioners to advance AI-driven fraud detection systems and enhance their deployment in real-world banking environments.

REFERENCES

Aggarwal, C. C., & Yu, P. S. (2001). Outlier detection for high dimensional data. *ACM SIGMOD Record*, *30*(2), 37-46. https://doi.org/10.1145/376284.375668

Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review*, *40*(NA), 100402-NA. https://doi.org/10.1016/j.cosrev.2021.100402

Alam, M. A., Sohel, A., Uddin, M. M., & Siddiki, A. (2024). Big Data And Chronic Disease Management Through Patient Monitoring And Treatment With Data Analytics. *Academic Journal on Artificial Intelligence, Machine Learning, Data Science and Management Information Systems*, *1*(01), 77-94.

https://doi.org/10.69593/ajaimldsmis.v1i01.133

Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms. *IEEE Access*, *10*(NA), 39700-39715. https://doi.org/10.1109/access.2022.3166891

Alhazmi, A. H., & Aljehane, N. O. (2020). A Survey Of Credit Card Fraud Detection Use Machine Learning. *2020 International Conference on Computing and Information Technology (ICCIT-1441)*, *NA*(NA), 1-6. https://doi.org/10.1109/iccit-144147971.2020.9213809

Ali, A., Abd Razak, S., 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), 9637-9637. https://doi.org/10.3390/app12199637

Ashtiani, M. N., & Raahemi, B. (2022). Intelligent Fraud Detection in Financial Statements using Machine Learning and Data Mining: A Systematic Literature Review. *IEEE Access*, *10*(NA), 72504-72525. https://doi.org/10.1109/access.2021.3096799

Bergh, C. M. M. R.-v. d., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime Science*, *7*(1), 5-NA. https://doi.org/10.1186/s40163-018-0079-3

Carter, E. (2020). Distort, Extort, Deceive and Exploit: Exploring the Inner Workings of a Romance Fraud. *The British Journal of Criminology*, *61*(2), 283-302. https://doi.org/10.1093/bjc/azaa072

Cheah, P. C. Y., Yang, Y., & Lee, B. G. (2023). Enhancing Financial Fraud Detection through Addressing Class Imbalance Using Hybrid SMOTE-GAN Techniques. *International Journal of Financial Studies*, *11*(3), 110-110. https://doi.org/10.3390/ijfs11030110

Chen, C., Liang, C., Lin, J., Wang, L., Liu, Z., Yang, X., Zhou, J., Shuang, Y., & Qi, Y. (2019). IEEE BigData - InfDetect: a Large Scale Graph-based Fraud Detection System for E-Commerce Insurance. *2019 IEEE International Conference on Big Data (Big Data)*, *NA*(NA), 1765-1773. https://doi.org/10.1109/bigdata47090.2019.9006115

Fang, W., Li, X., Zhou, P., Yan, J., Jiang, D., & Zhou, T. (2021). Deep Learning Anti-Fraud Model for Internet Loan: Where We Are Going. *IEEE Access*, *9*(NA), 9777-9784. https://doi.org/10.1109/access.2021.3051079

Hendri, N., & Sari, S. U. (2023). Sistematic Literature Review: The Strategy For Preventing Government Financial Report Fraud. *JAK (Jurnal Akuntansi) Kajian Ilmiah Akuntansi*, *10*(2), 323-336. https://doi.org/10.30656/jak.v10i2.6599

Hu, X., Chen, H., Chen, H., Li, X., Zhang, J., & Liu, S. (2023). Mining Mobile Network Fraudsters with Augmented Graph Neural Networks. *Entropy (Basel, Switzerland)*, *25*(1), 150-150. https://doi.org/10.3390/e25010150

Istiak, A., & Hwang, H. Y. (2024). Development of shape-memory polymer fiber reinforced epoxy composites for debondable adhesives. *Materials Today Communications*, *38*, 108015. https://doi.org/https://doi.org/10.1016/j.mtcomm.2023.108015

Istiak, A., Lee, H. G., & Hwang, H. Y. (2023). Characterization and Selection of Tailorable Heat Triggered Epoxy Shape Memory Polymers for Epoxy Debondable Adhesives. *Macromolecular Chemistry and Physics*, *224*(20), 2300241. https://doi.org/https://doi.org/10.1002/macp.202300241

Kapadiya, K., Patel, U., Gupta, R., Alshehri, M. D., Tanwar, S., Sharma, G., & Bokoro, P. N. (2022). Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: an Analysis, Architecture, and Future Prospects. *IEEE Access*, *10*(NA), 79606-79627. https://doi.org/10.1109/access.2022.3194569

Kurshan, E., Shen, H., & Yu, H. (2020). Financial Crime & Fraud Detection Using Graph Computing: Application Considerations & Outlook. *2020 Second International Conference on Transdisciplinary AI (TransAI)*, *NA*(NA), 125-130. https://doi.org/10.1109/transai49837.2020.00029

Doi: 10.70008/jmldeds.v1i01.53

Li, J., Chang, Y., Wang, Y., & Zhu, X. (2023). Tracking down financial statement fraud by analyzing the supplier-customer relationship network. *Computers & Industrial Engineering*, *178*(NA), 109118-109118. https://doi.org/10.1016/j.cie.2023.109118

Li, J., & Yang, D. (2023). Research on Financial Fraud Detection Models Integrating Multiple Relational Graphs. *Systems*, *11*(11), 539-539. https://doi.org/10.3390/systems11110539

Mazumder, M. S. A., Rahman, M. A., & Chakraborty, D. (2024). Patient Care and Financial Integrity In Healthcare Billing Through Advanced Fraud Detection Systems. *Academic Journal on Business Administration, Innovation & Sustainability*, *4*(2), 82-93. https://doi.org/10.69593/ajbais.v4i2.74

Md Samiul Alam, M. (2024). The Transformative Impact of Big Data in Healthcare: Improving Outcomes, Safety, and Efficiencies. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *3*(03), 01-12. https://doi.org/10.62304/jbedpm.v3i03.82

Mehbodniya, A., Alam, I., Pande, S., Neware, R., Rane, K. P., Shabaz, M., & Madhavan, M. V. (2021). Financial Fraud Detection in Healthcare Using Machine Learning and Deep Learning Techniques. *Security and Communication Networks*, *2021*(NA), 1-8. https://doi.org/10.1155/2021/9293877

Mosleuzzaman , M., Hussain, M. D., Shamsuzzaman, H. M., Mia, A., & Hossain, M. D. S. (2024). Electric Vehicle Powertrain Design: Innovations In Electrical Engineering. *Academic Journal on Innovation, Engineering & Emerging Technology*, *1*(01), 1-18. https://doi.org/10.69593/ajieet.v1i01.114

Mosleuzzaman, M., Shamsuzzaman, H. M., & Hussain, M. D. (2024). Engineering Challenges and Solutions in Smart Grid Integration with Electric Vehicles. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, *4*(03), 139-150. https://doi.org/10.69593/ajsteme.v4i03.102

Mosleuzzaman, M. D., Hussain, M. D., Shamsuzzaman, H. M., & Mia, A. (2024). Wireless Charging Technology for Electric Vehicles: Current Trends and Engineering Challenges. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *3*(04), 69-90. https://doi.org/10.62304/jieet.v3i04.205

Nicholls, J., Kuppa, A., & Le-Khac, N.-A. (2021). Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. *IEEE Access*, *9*, 163965-163986. https://doi.org/10.1109/access.2021.3134076

Ragazou, K., Passas, I., & Garefalakis, A. (2022). It Is Time for Anti-Bribery: Financial Institutions Set the New Strategic "Roadmap" to Mitigate Illicit Practices and Corruption in the Market. *Administrative Sciences*, *12*(4), 166-166. https://doi.org/10.3390/admsci12040166

Rahaman, M. A., Rozony, F. Z., Mazumder, M. S. A., & Haque, M. N. (2024). Big Data-Driven Decision Making in Project Management: A Comparative Analysis. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, *4*(03), 44-62. https://doi.org/10.69593/ajsteme.v4i03.88

Rahman, A. (2024a). Agile Project Management: Analyzing The Effectiveness of Agile Methodologies In It Projects Compared To Traditional Approaches. *Academic Journal on Business Administration, Innovation & Sustainability*, *4*(04), 53-69. https://doi.org/10.69593/ajbais.v4i04.127

Rahman, A. (2024c). IT Project Management Frameworks: Evaluating Best Practices and Methodologies for Successful IT Project Management. *Academic Journal on Artificial Intelligence, Machine Learning, Data Science and Management Information Systems*, *1*(01), 57-76. https://doi.org/10.69593/ajaimldsmis.v1i01.128

Rahman, A., Islam, M. R., Borna, R. S., & Saha, R. (2024). MIS Solutions During Natural Disaster Management: A Review On Responsiveness, Coordination, And Resource Allocation. *Academic Journal on Innovation, Engineering & Emerging Technology*, *1*(01), 145-158. https://doi.org/10.69593/ajieet.v1i01.145

Rahman, A., Saha, R., Goswami, D., & Mintoo, A. A. (2024). Climate Data Management Systems: Systematic Review Of Analytical Tools For Informing Policy Decisions. *Frontiers in*

Applied Engineering and Technology, *1*(01), 01-21. https://journal.aimintlllc.com/index.php/FAET/article/view/3

Reddy, G. D., Saxena, S., Tinggi, E. S., Isabels, K. R., Rathnakar, G., & Turar, U. (2022). Utilization of AI for Streamlining and Optimizing Credit Decision Process and Security Access Loan Risks in the Banking Sector. *2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA)*, *13*(NA), 1165-1171. https://doi.org/10.1109/icirca54612.2022.9985674

Saia, R., & Carta, S. (2019). Evaluating the benefits of using proactive transformed-domain-based techniques in fraud detection tasks. *Future Generation Computer Systems*, *93*(NA), 18-32. https://doi.org/10.1016/j.future.2018.10.016

Shamsuzzaman, H. M., Mosleuzzaman, M. D., Mia, A., & Nandi, A. (2024). Cybersecurity Risk Mitigation in Industrial Control Systems Analyzing Physical Hybrid And Virtual Test Bed Applications. *Academic Journal on Artificial Intelligence, Machine Learning, Data Science and Management Information Systems*, *1*(01), 19-39. https://doi.org/10.69593/ajaimldsmis.v1i01.123

Shamim, M. (2022). The Digital Leadership on Project Management in the Emerging Digital Era. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *1*(1), 1-14.

Sharma, A., & Panigrahi, P. K. (2012). A Review of Financial Accounting Fraud Detection based on Data Mining Techniques. *International Journal of Computer Applications*, *39*(1), 37-47. https://doi.org/10.5120/4787-7016

Shirodkar, N., Mandrekar, P., Mandrekar, R. S., Sakhalkar, R., Kumar, K. M. C., & Aswale, S. (2020). Credit Card Fraud Detection Techniques – A Survey. *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, *NA*(NA), 1-7. https://doi.org/10.1109/ic-etite47903.2020.112

Usman, A., Naveed, N., & Munawar, S. (2023). Intelligent Anti-Money Laundering Fraud Control Using Graph-Based Machine Learning Model for the Financial Domain. *Journal of Cases on Information Technology*, *25*(1), 1-20. https://doi.org/10.4018/jcit.316665

Wei, S., & Lee, S. (2024). Financial Anti-Fraud Based on Dual-Channel Graph Attention Network. *Journal of Theoretical and Applied Electronic Commerce Research*, *19*(1), 297-314. https://doi.org/10.3390/jtaer19010016