IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Systematic Review Of Artificial Intelligence Applications In Financial Fraud Detection

KrishnaPhani Mangi *, Sunil kumar Mangi**

*(Computerscience and Technology SDC College Osmania university)

** (jawaharlal nehru technological university, Hyderabad

Abstract:

Artificial Intelligence (AI) has transformed financial fraud detection by enabling more accurate, scalable, and adaptive systems across sectors such as banking, insurance, and healthcare. This systematic review examines the effectiveness of AI-based approaches in detecting financial fraud and explores the challenges and limitations associated with their implementation. Peer-reviewed studies from major academic databases were systematically analyzed, focusing on machine learning and deep learning techniques used to evaluate the performance of AI-driven fraud detection systems. The results demonstrate that AI significantly enhances real-time fraud detection and improves adaptability to evolving fraud patterns when compared to traditional rule-based methods. Despite these advantages, several challenges hinder widespread adoption, including ethical concerns, algorithmic bias, data privacy risks, system vulnerabilities, and scalability constraints—particularly for smaller organizations. Overall, AI-based fraud detection represents a transformative solution for combating financial fraud; however, realizing its full potential requires improved data quality, the development of explainable AI models, strengthened cybersecurity measures, and updated regulatory frameworks. Collaboration among policymakers and stakeholders is essential to ensure the ethical and effective deployment of AI in fraud detection.

Keywords — Artificial Intelligence; Fraud Detection; Machine Learning; Data Privacy; Algorithmic Bias; Financial Sector;Cybersecurity

I. INTRODUCTION

The rapid growth of digital financial transactions has significantly transformed global financial systems, offering improved efficiency, accessibility, and convenience. However, this digital transformation has also contributed to a substantial rise in financial fraud. Cybercriminals now employ sophisticated techniques such as identity theft, transaction manipulation, and cyber-enabled fraud schemes, which pose serious threats to financial institutions and consumers. Traditional fraud detection systems, largely based on static rules and manual monitoring, are increasingly ineffective in addressing these complex and evolving threats. As a result, there is a growing need for advanced technological solutions capable of enhancing financial security.

Artificial Intelligence (AI) has emerged as a powerful tool in financial fraud detection. By utilizing machine learning (ML) and deep learning (DL) algorithms, AI systems can analyze large volumes of transactional data to identify anomalies and detect fraudulent behavior in real time. Unlike conventional methods, AI-based systems are adaptive, enabling continuous learning from historical and new data. This adaptability allows organizations to respond effectively to emerging fraud patterns while reducing false positives and financial losses.

1.1 Role of Artificial Intelligence in Fraud Detection

1.2

AI-driven fraud detection systems offer significant advantages over traditional approaches. Machine learning models can uncover hidden patterns within complex datasets, while deep learning techniques are capable of processing high-dimensional and unstructured data. These capabilities allow AI systems to detect suspicious activities with greater accuracy and speed. Moreover, AI models can operate at scale, making them suitable for high-volume transaction environments such as banking, insurance, and digital payment platforms.

AI has been widely adopted across various sectors. In banking, AI systems monitor account activity to prevent unauthorized transactions. In insurance, AI assists in identifying fraudulent claims by analyzing inconsistencies in customer data. Similarly, in healthcare, AI-based solutions help detect billing fraud. These applications demonstrate AI's potential to enhance fraud detection efficiency and reliability across multiple industries.

1.3 Challenges and Ethical Considerations

1.4

Despite its benefits, the implementation of AI in fraud detection presents several challenges. Data quality remains a critical concern, as AI models depend on accurate and comprehensive datasets for reliable performance. Poor-quality data can lead to incorrect predictions, resulting in false positives or undetected fraud. Additionally, algorithmic bias poses ethical risks, as AI systems trained on historical data may unintentionally reinforce existing inequalities, leading to unfair outcomes for certain demographic groups.

Data privacy is another major challenge. AI-based fraud detection systems require access to sensitive personal and financial information, raising concerns about data protection and regulatory compliance. Ensuring transparency and explain ability in AI decision-making is essential to maintain trust and meet legal requirements.

1.3 Cyber security Risks and Study Significance

AI-based fraud detection systems are also vulnerable to cyber security threats, including adversarial attacks designed to manipulate AI models and evade detection. These risks highlight the need for robust cyber security measures to protect AI systems and maintain their integrity. Continuous monitoring and system updates are essential to counter evolving cyber threats.

This study aims to systematically review the effectiveness of AI-based fraud detection systems across various sectors. By examining recent literature, the study evaluates the benefits, limitations, and ethical implications of AI adoption in fraud detection. The findings contribute to a deeper understanding of how AI can be responsibly and effectively used to strengthen financial security in an increasingly digital financial landscape.

2. Methodology

This study adopts a systematic review methodology to critically examine the role of Artificial Intelligence (AI) in fraud detection within financial security. A structured and transparent review process was applied to ensure the rigorous selection of literature, accurate data extraction, and reliable synthesis of findings, in line with established guidelines for systematic reviews (Kitchenham et al., 2009). Such methodologies provide a robust framework for consolidating existing knowledge, identifying research trends, challenges, and gaps, and enhancing the credibility of conclusions drawn from prior studies (Dziopa & Ahern, 2011). The methodological approach was specifically designed to address the study's research questions by evaluating the effectiveness of AI-based fraud detection systems and the challenges associated with their implementation.

2.1. Search Strategy

An exhaustive search strategy was developed to capture a comprehensive body of academic literature on AI-driven fraud detection in the financial sector. Major academic databases, including Scopus, Web of Science, and IEEE Xplore, were systematically searched to identify relevant peer-reviewed studies (Cocchia, 2014). Search strings combined key terms such as artificial intelligence, fraud detection, financial security, machine learning, and deep learning, using Boolean operators (AND, OR) to maximize coverage while reducing irrelevant results.

The search was limited to studies published between 2020 and 2024 to reflect recent advancements in AI technologies and their applications in financial fraud detection (Lame, 2019). Only English-language publications were included to ensure consistency and reduce potential language-related bias. This process yielded an initial pool of approximately 500 documents for further screening (Torres-Carrión et al., 2018).

1) 2.2. Inclusion and Exclusion Criteria

To refine the initial dataset, predefined inclusion and exclusion criteria were applied. Studies were included if they were peer-reviewed and focused on the application of AI techniques—such as machine learning, neural networks, and natural language processing (NLP)—in financial fraud detection (Xiao & Watson, 2019). Preference was given to research that reported practical implementations or real-world case studies, as these provided direct insights into system performance and effectiveness (Vicente-Saez & Martinez-Fuentes, 2018).

Studies were excluded if they consisted of conference papers, editorials, white papers, or lacked empirical evidence. Additionally, articles that focused exclusively on theoretical AI models without addressing practical fraud detection applications were removed (Xiao & Watson, 2019). Following this screening process, the final sample was reduced to 145 high-quality and relevant studies (Vicente-Saez & Martinez-Fuentes, 2018).

2.3. Data Extraction and Synthesis

A systematic data extraction process was conducted for each selected study to collect relevant information, including the AI techniques employed, types of fraud addressed (e.g., credit card or insurance fraud), dataset characteristics, detection accuracy, and implementation challenges (Torres-Carrión et al., 2018). These parameters were chosen to ensure alignment with the study's objectives and to provide a comprehensive overview of AI applications in fraud detection (Lame, 2019).

The extracted data were synthesized using both quantitative and qualitative approaches. Bibliometric analysis was used to identify publication trends, commonly applied AI techniques, and dominant financial sectors adopting AI-based fraud detection (Bello et al., 2023). Thematic analysis was then conducted to explore recurring challenges and limitations, including data privacy concerns, ethical implications, and system vulnerabilities (Kaushik et al., 2024). Network analysis further supported the synthesis by examining relationships between AI methodologies and fraud detection outcomes, highlighting the evolution of deep learning approaches compared to traditional machine learning techniques across sectors such as banking, insurance, and retail (Sinha et al., 2022; Xu et al., 2024).

2.4. Addressing Bias and Ensuring Reliability

Several measures were implemented to minimize bias and enhance the reliability of the review. Data extraction was independently performed by two reviewers, with discrepancies resolved through consensus to reduce subjective bias (Budgen & Brereton, 2006). Each study was also evaluated using standardized quality assessment criteria, focusing on methodological rigor, data relevance, and applicability of findings (Johora et al., 2024).

A critical appraisal tool was employed to assess potential sources of bias, including selection, measurement, and reporting bias (Mohammed & Rahman, 2024). These procedures ensured that the findings were grounded in high-quality evidence and that the conclusions drawn were both reliable and transparent (Hassan et al., 2023).

Overall, this systematic review followed a rigorous and transparent methodological framework to evaluate the role of AI in financial fraud detection. By combining a structured search strategy, strict selection criteria, and multiple synthesis techniques, the study provides a comprehensive assessment of current AI-based fraud detection systems. Measures taken to reduce bias further strengthen the validity and real-world applicability of the findings, contributing valuable insights to the growing literature on AI-driven financial security (Budgen & Brereton, 2006; Xu et al., 2024).

3. Analyses and Findings

3.1. Research Methods Employed in Previous Studies

The research methods adopted in the analyzed literature demonstrate a diverse and comprehensive examination of artificial intelligence (AI) applications in fraud detection and cybersecurity. A substantial proportion of the reviewed studies employ quantitative research methods, with a strong emphasis on machine learning and deep learning techniques. These studies typically rely on empirical data analysis, statistical modeling, and performance evaluation to assess the effectiveness of AI-based fraud detection systems.

For example, Mohanty and Mishra (2023) evaluated AI-driven fraud detection solutions in the financial sector, highlighting the effectiveness of platforms such as Teradata and Riskified. Their quantitative approach, grounded in empirical performance metrics, contributes significantly to understanding AI's role in mitigating fraud within banking and financial services.

Comparative research methods also feature prominently in the literature. Zanke (2023), for instance, conducted a comparative analysis across banking, insurance, and healthcare sectors to assess the scalability and performance of AI-driven fraud detection systems. Such studies provide valuable insights into sector-specific challenges and underscore the importance of tailoring AI models to distinct regulatory and operational environments.

Another methodological stream focuses on cybersecurity-oriented approaches, where AI is integrated into network security frameworks. Mishra (2023) emphasized the use of techniques such as the Enhanced Encryption Standard (EES) and K-Nearest Neighbor (KNN) algorithms to protect financial systems against cyber threats. This approach reflects a growing trend in which fraud detection research extends beyond transactional fraud to encompass broader cybersecurity risks.

Deep learning methodologies are also widely explored, particularly in studies addressing complex transactional environments. Xu et al. (2024) applied Autoencoder-based deep learning models to credit card fraud detection, achieving notable improvements in detection accuracy. These approaches demonstrate AI's capacity to identify subtle anomalies within large-scale datasets, reinforcing its suitability for high-volume financial systems.

In addition, systematic literature reviews form an important methodological category. Sood et al. (2023) conducted a large-scale systematic review and network analysis of AI-based fraud detection research spanning two decades. Using tools such as VOSviewer and K-means clustering, the study identified key research trends and gaps, offering a macro-level perspective that supports future investigations.

Emerging research has also introduced novel AI architectures, including Graph Neural Networks (GNNs), Generative Adversarial Networks (GANs), and Temporal Convolutional Networks (TCNs). Kuttiyappan and Rajasekar (2024) evaluated these advanced models, demonstrating their superiority over traditional rule-based systems and emphasizing the shift toward adaptive and self-learning fraud detection mechanisms.

Finally, mixed-method research designs are evident in studies such as Mohammed and Rahman (2024), who combined surveys, interviews, and case studies to examine AI adoption in fraud detection within Saudi Arabia's private sector. This approach enriched the analysis by integrating quantitative findings with contextual qualitative insights, highlighting the importance of national and institutional factors.

Overall, the reviewed studies employ a wide range of quantitative, qualitative, and mixed methodologies, reflecting the complexity of AI-driven fraud detection and the need for multidimensional research approaches.

3.2. Theoretical Foundations in AI-Based Fraud Detection Research

The analyzed literature is grounded in a variety of theoretical frameworks that inform both the design and application of AI-based fraud detection systems. Machine learning theory serves as a foundational framework across many studies, emphasizing the ability of AI systems to learn from historical data and improve predictive accuracy over time. Mohanty and Mishra (2023) demonstrated how machine learning models adapt to evolving fraud patterns, offering advantages over static rule-based systems.

Closely related, deep learning theory underpins studies that address complex and high-dimensional datasets. Xu et al. (2024) employed deep neural networks to detect credit card fraud, illustrating how multi-layer architectures can identify intricate transactional patterns that simpler models often miss. This theoretical approach is particularly relevant in large-scale financial environments where data complexity is high.

Anomaly detection theory is another widely applied framework, based on the assumption that fraudulent activities deviate from normal behavioral patterns. Zanke (2023) utilized this theory to explain how AI systems detect irregularities across multiple sectors, reinforcing its value in real-time fraud monitoring.

The application of natural language processing (NLP) theory is evident in studies focused on identity verification and customer communication analysis. Hassan et al. (2023) applied NLP techniques to enhance Know Your Customer (KYC) processes, demonstrating how unstructured textual data can be leveraged to detect fraudulent behavior and phishing attempts.

Ethical considerations are framed through data ethics and fairness theories, particularly in studies addressing bias, transparency, and accountability. Kaushik et al. (2024) emphasized the importance of ethical frameworks in ensuring responsible AI deployment, especially when handling sensitive financial data.

The theory of adversarial machine learning is increasingly relevant in addressing AI vulnerabilities. Roshanaei et al. (2024) explored how attackers manipulate AI models through adversarial inputs, highlighting the need for robust and resilient system design.

Additional theoretical perspectives include cybersecurity and risk management frameworks, which integrate AI into multi-layered defense strategies (Bello et al., 2023), behavioral biometrics theory, which analyzes user interaction patterns for fraud detection (Sood et al., 2023), and graph theory, which enables the visualization of transactional relationships to uncover complex fraud networks (Hassan et al., 2023).

Finally, self-learning systems theory emphasizes AI adaptability. Kuttiyappan and Rajasekar (2024) highlighted the importance of continuously updating models to counter evolving fraud tactics, ensuring long-term system effectiveness.

3.3. Effectiveness of AI-Based Techniques Across Financial Sectors

The reviewed studies consistently demonstrate that AI-based techniques significantly enhance fraud detection across various sectors, including banking, insurance, and healthcare. In the banking sector, Mohanty and Mishra (2023) reported substantial reductions in fraud incidents through the use of AI platforms capable of real-time transaction monitoring.

Comparative studies, such as Zanke (2023), further highlighted AI's adaptability across sectors. In healthcare, AI-based anomaly detection and deep learning models proved particularly effective in identifying fraudulent insurance claims, while in banking and insurance, machine learning algorithms improved detection accuracy and response times.

Deep learning approaches, especially Autoencoder models, have shown superior performance in credit card fraud detection by identifying hidden patterns in transactional data (Xu et al., 2024). Similarly, graph analytics have proven effective in insurance and money laundering detection by mapping complex relationships between entities (Hassan et al., 2023).

Despite these successes, challenges remain. Mishra (2023) noted that advanced cyber threats can undermine traditional AI models, emphasizing the need for continuous system updates. Mohammed and Rahman (2024) further highlighted that AI effectiveness is closely linked to data quality and availability.

Ethical considerations also influence effectiveness, as biased or opaque models can erode stakeholder trust (Kaushik et al., 2024). Adaptability, particularly through self-learning systems, has emerged as a critical factor in maintaining long-term effectiveness (Kuttiyappan & Rajasekar, 2024).

3.4. Challenges and Limitations of AI-Based Fraud Detection Systems

Despite their advantages, AI-based fraud detection systems face several notable challenges. Ethical concerns, including algorithmic bias and lack of transparency, pose significant risks, particularly when models are trained on biased datasets (Kaushik et al., 2024).

Data privacy and regulatory compliance represent another major limitation. The reliance on large volumes of sensitive data raises concerns under regulations such as GDPR, complicating AI implementation while maintaining system performance (Hassan et al., 2023).

AI systems are also vulnerable to adversarial attacks, where malicious actors manipulate input data to bypass detection mechanisms (Mishra, 2023). This highlights the need for robust defenses and continuous model updates.

Scalability and cost barriers further restrict adoption, especially for smaller institutions and organizations in developing economies. Mohammed and Rahman (2024) emphasized that limited resources and technical expertise hinder widespread implementation.

The lack of explainability in advanced AI models, particularly deep learning systems, remains a critical issue. Xu et al. (2024) noted that “black-box” models complicate accountability and regulatory acceptance.

Additional challenges include data quality issues, surveillance-related ethical concerns, integration with legacy systems, and uncertain regulatory frameworks (Bello et al., 2023; Roshanaei et al., 2024).

4. Discussion of Findings

This section critically discusses the findings of the systematic review, focusing on the effectiveness of AI-based fraud detection systems and the challenges associated with their implementation across financial sectors. The reviewed literature demonstrates that AI has significantly transformed fraud detection by enabling faster, more accurate, and adaptive systems. However, ethical, technical, and regulatory barriers continue to limit the full realization of AI's potential. The discussion below synthesizes these findings and situates them within the broader context of financial security and AI adoption.

4.1. Effectiveness of AI-Based Fraud Detection Systems

The findings consistently indicate that AI-based techniques outperform traditional rule-based systems in detecting financial fraud. One of the most significant advantages of AI lies in its real-time detection capability. As demonstrated by Mohanty and Mishra (2023), AI platforms such as Teradata and Feedzai can process large volumes of transactional data instantaneously, allowing financial institutions to identify and respond to fraudulent activities with minimal delay. This capability is particularly critical in the banking sector, where fraud can occur within seconds and delayed detection often results in substantial financial losses.

Another key strength of AI-based systems is their adaptive learning capability. Unlike traditional systems that rely on static rules, AI models learn from historical data and continuously refine their detection mechanisms. Xu et al. (2024) showed that deep learning models, particularly Autoencoder algorithms, achieved superior performance in identifying complex fraud patterns in credit card transactions. This adaptability enables AI systems to remain effective even as fraud strategies evolve, highlighting their long-term value in dynamic financial environments.

4.2. Scalability and Cross-Sector Applicability of AI

The review also highlights AI's scalability and versatility across multiple sectors, including banking, insurance, and healthcare. Zanke (2023) demonstrated that AI-driven fraud detection systems effectively handle large and complex datasets, making them particularly suitable for data-intensive sectors. In healthcare, AI systems detect fraudulent insurance claims by identifying anomalies in billing patterns, while in banking, they identify suspicious transactions associated with money laundering and account takeovers.

These findings emphasize that AI techniques—particularly machine learning, anomaly detection, and deep learning—can be adapted to different industry contexts with relatively minor modifications. This cross-sector applicability underscores AI's role as a flexible and scalable solution for fraud detection, capable of addressing sector-specific risks while maintaining high levels of accuracy.

4.3. Data Dependency and Its Impact on System Performance

Despite the strong performance of AI-based systems, the review reveals that their effectiveness is highly dependent on data quality. Sood et al. (2023) emphasized that AI models require large volumes of accurate, complete, and up-to-date data to function effectively. When training data is noisy, incomplete, or outdated, AI systems are more likely to generate false positives or false negatives.

This limitation is particularly concerning in high-risk financial environments, where incorrect fraud alerts can disrupt customer experiences, increase operational costs, and undermine trust. Consequently, the findings suggest that AI-based fraud detection should be complemented by robust data governance frameworks to ensure data integrity and reliability.

4.4. Ethical Challenges: Bias, Fairness, and Transparency

Ethical concerns emerge as a major challenge in the deployment of AI-based fraud detection systems. Kaushik et al. (2024) highlighted the risk of algorithmic bias, particularly when AI models are trained on datasets that reflect existing social or institutional biases. In financial services, biased models may disproportionately target certain demographic groups, leading to unfair treatment and potential legal consequences.

Additionally, the lack of transparency and explainability in complex AI systems—especially deep learning models—poses a significant challenge. When stakeholders cannot understand how decisions are made, trust in AI systems diminishes. This issue is especially critical in fraud detection, where incorrect decisions can have serious financial and reputational implications. The findings suggest that improving explainability is essential for ethical compliance, regulatory acceptance, and user trust.

4.5. Data Privacy and Regulatory Constraints

Data privacy concerns further complicate the implementation of AI-based fraud detection systems. Hassan et al. (2023) noted that AI systems require access to extensive personal and financial data, raising concerns about data collection, storage, and usage. Regulatory frameworks such as the General Data Protection Regulation (GDPR) impose strict limitations on data access, which can restrict AI model performance.

This creates a fundamental tension between data accessibility and privacy protection. While comprehensive datasets enhance fraud detection accuracy, excessive data collection increases the risk of misuse and data breaches. The findings suggest that organizations must strike a careful balance by adopting privacy-preserving techniques while maintaining sufficient data access for effective fraud detection.

4.6. System Vulnerabilities and Adversarial Threats

The review also identifies system vulnerabilities as a critical limitation of AI-based fraud detection. Mishra (2023) highlighted the growing threat of adversarial attacks, where fraudsters manipulate input data to deceive AI models. As cybercriminals increasingly adopt AI-driven techniques, the risk of AI systems being exploited also increases.

These vulnerabilities highlight the need for continuous monitoring, regular model updates, and the integration of advanced cybersecurity measures. However, such safeguards require substantial investment, which may not be feasible for all organizations. This reinforces the idea that AI-based fraud detection is not a standalone solution but must be part of a broader cybersecurity strategy.

4.7. Scalability and Resource Constraints

Scalability remains a significant challenge, particularly for smaller financial institutions and organizations in developing regions. Mohammed and Rahman (2024) emphasized that the high costs associated with AI infrastructure, skilled personnel, and system maintenance limit widespread adoption. While large institutions can absorb these costs, smaller organizations often lack the necessary resources and technical expertise.

As a result, the benefits of AI-based fraud detection are unevenly distributed, creating disparities in fraud prevention capabilities across regions and institutions. Addressing this issue requires the development of cost-effective AI solutions, cloud-based platforms, and capacity-building initiatives to support broader adoption.

4.8. Regulatory and Compliance Challenges

Regulatory uncertainty further complicates AI implementation in fraud detection. Bello et al. (2023) noted that regulatory frameworks have struggled to keep pace with rapid AI advancements. Outdated or ambiguous regulations create compliance challenges, particularly for institutions operating across multiple jurisdictions.

The lack of standardized global regulations exacerbates this issue, forcing organizations to navigate conflicting legal requirements. The findings suggest that closer collaboration between regulators, policymakers, and industry stakeholders is essential to develop adaptive regulatory frameworks that reflect the realities of AI-based fraud detection systems.

5. CONCLUSION AND RECOMMENDATIONS

This systematic review has examined the effectiveness of artificial intelligence (AI)–based techniques in financial fraud detection across multiple sectors, alongside the challenges associated with their implementation. The findings indicate that AI technologies, particularly machine learning and deep learning approaches, have significantly enhanced the ability to detect fraudulent activities by enabling real-time analysis, processing large volumes of data, and adapting to continuously evolving fraud strategies. Across sectors such as banking, healthcare, and insurance, AI-based systems consistently outperform traditional rule-based and manual fraud detection methods. Studies by Zanke (2023) and Mohanty and Mishra (2023) demonstrate that AI-driven solutions improve detection accuracy, reduce response time, and substantially minimize financial losses by uncovering complex patterns that are often overlooked by human analysts.

Despite these advantages, the review also highlights several critical challenges that limit the full potential of AI-based fraud detection systems. Ethical concerns, particularly those related to algorithmic bias and the lack of transparency in AI decision-making, remain significant obstacles. As emphasized by Kaushik et al. (2024), biased training data can lead to unfair outcomes, undermining trust in AI systems and raising concerns about accountability in financial decision-making. Additionally, data privacy constraints and system vulnerabilities pose serious risks to the reliability and security of AI-driven solutions. Mishra (2023) noted that adversarial attacks and the threat of data breaches can compromise AI models, especially as fraudsters increasingly leverage advanced technologies to exploit system weaknesses. Furthermore, scalability remains a major concern, particularly for smaller institutions and organizations in developing regions that often lack the financial resources, infrastructure, and technical expertise required to deploy and maintain AI-based systems effectively.

In summary, AI-based techniques represent a transformative advancement in financial fraud detection, offering clear improvements over traditional approaches. However, their long-term success depends on addressing ethical, technical, and regulatory challenges that currently constrain widespread adoption. As AI technologies continue to evolve, their role in combating financial fraud is expected to expand, provided that continuous innovation and cross-sector collaboration are maintained.

Recommendations

Based on the findings of this review, several recommendations are proposed to enhance the effectiveness and responsible deployment of AI-based fraud detection systems.

First, organizations should prioritize the improvement of data quality used for training AI models. As highlighted by Sood et al. (2023), AI systems are highly dependent on accurate, comprehensive, and unbiased datasets. Poor-quality or incomplete data can lead to false positives and false negatives, reducing system reliability. Regular data audits and continuous updates to training datasets are essential to ensure that AI models remain responsive to emerging fraud patterns.

Second, to mitigate concerns related to algorithmic bias and transparency, financial institutions should invest in the development and adoption of explainable AI (XAI) models. Xu et al. (2024) noted that many deep learning models function as "black boxes," making it difficult to interpret or justify their decisions. Explainable AI can improve transparency, enhance user trust, and support compliance with regulatory requirements related to fairness and accountability.

Third, strengthening cybersecurity measures is critical to protecting AI-based fraud detection systems from adversarial attacks and data breaches. As fraud techniques become increasingly sophisticated, organizations must implement continuous monitoring, adversarial training, and robust threat detection mechanisms. Mishra (2023) emphasized the need to integrate AI systems with advanced cybersecurity frameworks and to provide regular cybersecurity training for personnel responsible for managing these technologies.

To address scalability challenges, particularly for smaller institutions and organizations in developing markets, the adoption of cloud-based AI solutions and AI-as-a-Service (AIaaS) models is strongly recommended. These solutions offer cost-effective, flexible, and scalable alternatives to traditional on-premise systems. Mohammed and Rahman (2024) noted that cloud-based platforms can significantly reduce infrastructure costs while enabling broader access to AI capabilities. In addition, collaboration between governments, financial institutions, and industry stakeholders is essential to support capacity-building initiatives and develop technical expertise in under-resourced regions.

Finally, there is an urgent need for updated and harmonized regulatory frameworks that reflect the unique characteristics of AI-based fraud detection systems. Bello et al. (2023) highlighted the regulatory uncertainty faced by institutions due to outdated or fragmented guidelines. Policymakers should work closely with industry stakeholders to establish regulations that promote ethical AI use, safeguard data privacy, and ensure accountability, while simultaneously encouraging innovation.

Limitations of the Study

Although this systematic review provides valuable insights into AI-based fraud detection, several limitations should be acknowledged. First, the review relied primarily on secondary data from existing literature, which may not fully capture the most recent developments in AI technologies. Given the rapid pace of innovation in this field, some emerging techniques may not yet be reflected in published studies.

Second, the focus on English-language publications may introduce language bias and limit the generalizability of the findings to non-English-speaking regions. Future research should incorporate studies published in other languages to provide a more comprehensive global perspective.

Finally, the review did not extensively examine sector-specific differences that may influence the implementation and performance of AI systems. While the findings demonstrate the effectiveness of AI across multiple sectors, each industry faces distinct regulatory, operational, and ethical challenges. Future studies should conduct in-depth, sector-specific analyses to develop more targeted recommendations for AI-based fraud detection.

Despite these limitations, this review offers a comprehensive and critical assessment of the role of AI in financial fraud detection. By addressing the identified challenges and implementing the proposed recommendations, organizations can enhance the effectiveness, fairness, and sustainability of AI-based fraud detection systems, strengthening their ability to combat financial fraud in an increasingly complex digital environment.

ACKNOWLEDGMENT

We would like to express sincere gratitude to Dr N Chandrasekhar Nath and our organization successful completion of this study. Special appreciation is extended to the academic supervisors and mentors for their valuable guidance, constructive feedback, and continuous support throughout the research process. Their insights and expertise were instrumental in shaping the direction and quality of this work.

REFERENCES

• Adhikari, P., & Hamal, P. (2024). Impact and regulations of artificial intelligence on the labor market and employment in the USA.

• Ahmad, K., Maabreh, M., Ghaly, M., Khan, K., Qadir, J., & Al-Fuqaha, A. (2022). Developing future human-centered smart cities: Critical analysis of smart city security, data management, and ethical challenges. Computer Science Review, 43, 100452.

• Al-Dosari, K., Fetais, N., & Kucukvar, M. (2024). Artificial intelligence and cyber defense systems for the banking industry: A qualitative study of AI applications and challenges. Cybernetics and Systems, 55(2), 302–330.

• Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2023). Re-thinking data strategy and integration for artificial intelligence: Concepts, opportunities, and challenges. Applied Sciences, 13(12), 7082.

• Al-Fatlawi, A., Al-Khazaali, A. A. T., & Hasan, S. H. (2024). AI-based model for fraud detection in banking systems. Journal of Fusion: Practice and Applications, 14(1), 19–27.

• Ali, G., Mijwil, M. M., Buruga, B. A., Abotaleb, M., & Adamopoulos, I. (2024). A survey on artificial intelligence in cybersecurity for smart agriculture: State-of-the-art, cyber threats, applications, and ethical concerns. Mesopotamian Journal of Computer Science, 71–121.

• Al-Mansoori, S., & Salem, M. B. (2023). The role of artificial intelligence and machine learning in shaping the future of cybersecurity: Trends, applications, and ethical considerations. International Journal of Social Analytics, 8(9), 1–16.

• Bello, O. A., Folorunso, A., Onwuchekwa, J., & Ejiofor, O. E. (2023). A comprehensive framework for strengthening U.S. financial cybersecurity: Integrating machine learning and AI in fraud detection systems. European Journal of Computer Science and Information Technology, 11(6), 62–83.

• Budgen, D., & Brereton, P. (2006). Performing systematic literature reviews in software engineering. In Proceedings of the 28th International Conference on Software Engineering (pp. 1051–1052).

• Cocchia, A. (2014). Smart and digital city: A systematic literature review. In Smart City: How to Create Public and Economic Value with High Technology in Urban Space (pp. 13–43).

• Dhayanidhi, G. (2022). Research on IoT threats and implementation of AI/ML to address emerging cybersecurity issues in IoT with cloud computing.

• Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: A review. Sensors, 23(3), 1151.

• Dziopa, F., & Ahern, K. (2011). A systematic literature review of the applications of Q-technique and its methodology. Methodology.

• Familoni, B. T. (2024). Cybersecurity challenges in the age of AI: Theoretical approaches and practical solutions. Computer Science & IT Research Journal, 5(3), 703–724.

• Hassan, M., Aziz, L. A. R., & Andriansyah, Y. (2023). The role of artificial intelligence in modern banking: AI-driven approaches for fraud prevention, risk management, and regulatory compliance. Reviews of Contemporary Business Analytics, 6(1), 110–132.

• Johora, F. T., Hasan, R., Farabi, S. F., Akter, J., & Al Mahmud, M. A. (2024). AI-powered fraud detection in banking: Safeguarding financial transactions. American Journal of Management and Economics Innovations, 6(6), 8–22.

• Kalla, D., & Kuraku, S. (2023). Advantages, disadvantages, and risks associated with ChatGPT and AI in cybersecurity. Journal of Emerging Technologies and Innovative Research, 10(10).

• Kaushik, K., Khan, A., Kumari, A., Sharma, I., & Dubey, R. (2024). Ethical considerations in AI-based cybersecurity. In Next-Generation Cybersecurity: AI, ML, and Blockchain (pp. 437–470). Springer.

• Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering. Information and Software Technology, 51(1), 7–15.

• Kuttiyappan, D., & Rajasekar, V. (2024). AI-enhanced fraud detection: Novel approaches and performance analysis. In Proceedings of the International Conference on Artificial Intelligence, Communication, IoT, Data Engineering and Security.

• Lame, G. (2019). Systematic literature reviews: An introduction. In Proceedings of the Design Society: International Conference on Engineering Design (pp. 1633–1642). Cambridge University Press.

• Mishra, S. (2023). Exploring the impact of AI-based cybersecurity in financial sector management. Applied Sciences, 13(10), 5875.

• Mohammed, A. F. A., & Rahman, H. M. A. A. (2024). The role of artificial intelligence in fraud detection in the private sector in Saudi Arabia.

• Mohanty, B., & Mishra, S. (2023). Role of artificial intelligence in financial fraud detection. Academy of Marketing Studies Journal, 27(S4).

• Nair, M. M., Deshmukh, A., & Tyagi, A. K. (2024). Artificial intelligence for cybersecurity: Current trends and future challenges. In Automated Secure Computing for Next-Generation Systems (pp. 83–114).

• Roshanaei, M., Khan, M. R., & Sylvester, N. N. (2024). Enhancing cybersecurity through AI and ML: Strategies, challenges, and future directions. Journal of Information Security, 15(3), 320–339.

• Sinha, M., Chacko, E., & Makhija, P. (2022). AI-based technologies for digital and banking fraud during COVID-19. In Integrating Meta-Heuristics and Machine Learning for Real-World Optimization Problems (pp. 443–459). Springer.

• Sontan, A. D., & Samuel, S. V. (2024). The intersection of artificial intelligence and cybersecurity: Challenges and opportunities. World Journal of Advanced Research and Reviews, 21(2), 1720–1736.

• Sood, P., Sharma, C., Nijjer, S., & Sakhuja, S. (2023). Role of artificial intelligence in detecting and preventing financial fraud using natural language processing. International Journal of System Assurance Engineering and Management, 14(6), 2120–2135.

• Torres-Carrión, P. V., González-González, C. S., Aciar, S., & Rodríguez-Morales, G. (2018). Methodology for systematic literature review applied to engineering and education. In IEEE Global Engineering Education Conference (pp. 1364–1373).

• Veluru, C. S. (2024). Responsible artificial intelligence on large-scale data to prevent misuse, unethical challenges, and security breaches. Journal of Artificial Intelligence & Cloud Computing.

• Vicente-Saez, R., & Martinez-Fuentes, C. (2018). Open science now: A systematic literature review for an integrated definition. Journal of Business Research, 88, 428–436.

• Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. Journal of Planning Education and Research, 39(1), 93–112.

• Xu, J., Yang, T., Zhuang, S., Li, H., & Lu, W. (2024). AI-based financial transaction monitoring and fraud prevention with behaviour prediction.

• Zanke, P. (2023). AI-driven fraud detection systems: A comparative study across banking, insurance, and healthcare. Advances in Deep Learning Techniques, 3(2), 1–22.