IJSRA

International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(Review Article)

Check for updates

AI-powered fraud detection in digital banking: Enhancing security through machine learning

David A Oduro [1, *], Joy Nnenna Okolo [2], Adepeju Deborah Bello [3], Ayodeji Temitope Ajibade [4], Abiodun Muritala Fatomi [5], Tunmise Suliat Oyekola [6] and Soyingbe Folashade Owoo-Adebayo [7]

[1] *Independence Researcher, Compliance, JP Morgan Chase & Co, U.S.A.*
[2] *Department of Computer Science, South Dakota State University.*
[3] *Independent Researcher, Fraud Analyst, Barclays U.K.*
[4] *Independent Researcher, Fraud Analyst, Barclays U.K.*
[5] *Department of Information Technology, Estuary Business Solution (MTN).*
[6] *Department of Software Engineering, Gloqal Inc.*
[7] *Department of Finance, Lagos State University, Nigeria.*

International Journal of Science and Research Archive, 2025, 14(03), 1412-1420

Publication history: Received on 16 February 2025; revised on 23 March 2025; accepted on 26 March 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.14.3.0854

Abstract

This study examines the role of Artificial Intelligence (AI) and Machine Learning (ML) in enhancing fraud detection within the digital banking sector. With financial transactions migrating to the digital platforms, sophistication of the fraudsters comes in and advanced security measures are needed. Machine Learning models that support the AI driven fraud detection systems, analyse huge datasets, find the anomalies and reduce the risk of financial fraud. In this literature review, this author critically evaluates existing AI/ML based fraud detection methods in terms of the effectiveness of the methods, the challenges faced by the methods, and avenues of what is scaled up more towards them being a solution. The review identifies key trends on supervised and unsupervised learning, deep learning models, and the findings on the anomaly detection technique. The findings highlight AI's capacity for enhancing the accuracy of fraud detection whilst tackling algorithmic bias, the privacy of data and the attack of adversarial. The study ends by providing recommendations for enhancing the fraud detection system in terms of the use of Explainable AI (XAI), real time fraud monitoring, and integrating blockchain into digital banking security.

Keywords: AI-powered fraud detection; Machine learning; Anomaly detection; Cybersecurity and Explainable AI (XAI)

1. Introduction

Digital banking plays a vital role in the evolution of the financial industry as a source of enabling financial inclusion in times of changed logistics of financial services delivery. The transformation is hinged on the democratization of banking facilities that internet banking services have brought, that have made banking easier, faster, and more convenient than ever. Digital banking is impactful because not only can it bring higher service delivery but it has the real potential of integrating the excluded, unbanked and underserved also into the formal financial ecosystem. Clearly, the rapid growth of digital banking has completely revolutionized financial services and have made things an easier affair. Nevertheless, cyber fraud risk has also increased to a level that can bring about substantial financial and reputational loss for institutions and customers. The major challenges to fully utilizing the incentive of digital banking are digital literacy, cybersecurity concerns and a need for strong regulatory framework. Machine learning can be used to play a major role in enhancing user data and fraud detection security in order to reduce these challenges [1].

[*] Corresponding author: David A Oduro

Copyright © 2025 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

Typically, traditional fraud detection systems (e.g., predefined rules, historical data) are not as sophisticated to encompass the types of frauds posed against them. Manual detection through traditional methods is time consuming, expensive and inaccurate, and, in big data age, it is impractical. However, these approaches, which mostly employed manual techniques of auditing, can be inefficient and unreliable because of the complexity of the problem. On the other hand, machine learning based security enhancement provides much more benefits, because these sophisticated methods can certainly process large data sets and can detect commonalities that may not be noticed by manual methods. Bello, & Olufemi, (2024) [2] opined that Artificial Intelligence (AI) can provide innovative solutions to this growing problem because of its capability to analyze large amounts of data, find patterns, and predict with high accuracy the fraudulent behavior. In particular, data mining-based approaches have been useful for their ability to find small irregularities in great volumes of data, thereby they are better in the accuracy and effectiveness of fraud detection [3]. It has caused integration of the AI and ML technologies and it has come up with proactive and adaptive solutions in detecting the fraudulent activities. The research task is based on a literature review approach of the potential of AI/ML tools for improving fraud detection in digital banking.

2. Methodology

This systematic review employs a comprehensive methodological framework to critically review and compare current practice and outcomes of the use of AI powered fraud detection in digital banking. The main objective is to evaluate how machine learning (ML) technologies improve security and reduce fraud risks on digital banking systems. This overview provides description of data sourcing, search strategy, and then study selection criteria to provide a comprehensive yet unbiased impression of what has been reported in the literature. The sources of primary data for this review are peer reviewed journal articles. A systematic search was conducted in the multiple academic databases such as Google Scholar, IEEE Xplore, ScienceDirect and SpringerLink. The search involved keywords like AI fraud detection, machine learning in digital banking, cybersecurity in financial institutions, fraud prevention technologies and AI based transaction monitoring. For the purpose of collecting recent advances on AI and ML applications to detect fraud, reviews were restricted to English language publications from 2010 to the present. Relevance to the objectives of the review, methodological rigor, and the advancement of our understanding about how the use of AI and ML technologies enhances fraud detection in digital banking was used as the basis of selection of the studies. Empirical research, theoretical frameworks, technical case studies and industry reports that investigate how AI can be used to enhance the effectiveness, challenges and applied practice of the fraud detection systems were included as inclusion criteria. On the other hand, studies that were excluded due to exclusion criteria were chosen that were not directly related to AI based fraud detection or were insufficient methodologically. The review follows this systematic methodology to help the reader to have a complete and informed review of how Artificial Intelligence and Machine Learning technologies are changing fraud detection in the digital banking. The findings aim to provide insights that will be of value to the financial institutions, to the regulatory bodies and to the technology developers to help them secure their digital finance and fight the frauds in the new digital finance.

3. Theoretical Framework

3.1. Anomaly Detection Theory:

Anomaly Detection Theory is a basic approach used for detecting fraudulent transactions which is to identify unusual pattern or behavior that deviates from the norm [4]. In the world of digital banking, anomalies are often fraudulent activities, including irregular transaction volumes, unusual login locations, quick changes in spending habits or unusual account activity patterns [5]. According to [2], in Digital banking, Anomaly Detection are used to detect new fraudulent schemes via identifying the outliers in transaction data that do not satisfy the expected behavior. The core problem of isolating these irregularities from big datasets is this theory and it helps financial institutions detect potential frauds proactively before significant damage is done. Anomaly detection has been used widely in different domains such as credit card fraud detection, insurance claims analysis, healthcare monitoring and cybersecurity intrusion detection [4]. The integration of anomaly detection in the fraud prevention systems allows banks to minimize false positives and at the same time increase probability of identification of real fraudulent activities.

3.2. Machine Learning Decision Framework:

Fraud detection and prevention has been revolutionized by AI techniques like machine learning (ML), deep learning and natural language processing (NLP). Supervised learning models such as decision trees and neural network are widely used to learn these fraudulent transactions based on the historical data by using machine learning algorithms. Using these models, it will be possible to distinguish between genuine and fraudulent transaction as such legitimate transactions can be discriminated from billiard by recognizing the subtle patterns which will not be detected by simple rule-based systems. As stated by [2], deep learning, a part of machine learning, has been extremely promising in fraud detection since it can process and analyze unstructured data such as images, text, or voice. On applications including credit card fraud detection, anti-money laundering (AML), CNNs and RNNs are used to attain techniques. Natural language process helps to detect the fraudulent activity through processing the textual data like the email and the captured description of the transaction to find the suspicious language and the pattern in it. Fraud prevention goes way beyond detection, it also involves proactive measures where AI is being applied. AI enables prediction of possible fraud hot spots for organizations to then implement preventative strategies to combat the occurrence. With the help of AI, the real time monitoring systems give instant alert on the suspicious activities which enables prompt step to counter fraud. These frameworks provide a foundation for understanding how AI and ML technologies enhance fraud detection capabilities in digital banking.

4. Literature Review

4.1. Fraud in Digital Banking

Fraud in digital banking, a broader concept that encompasses internet banking, involves fraudulent activities across various digital financial platforms, including online banking, mobile banking, and digital payment systems [6]. Fraudsters may employ various tactics such as hacking, phishing emails or websites, unsecured logins, website cloning, or data theft, targeting both internet banking users and other digital financial services. According to [7], Financial services institutions which are usually targets of cyber-fraudsters suffer from multifarious malware attacks in form of online phishing, keystroke-loggings malwares, and identity theft. Fraud in digital banking has evolved from simple phishing schemes to sophisticated, multi-layered attacks that exploit advanced technologies and social engineering techniques. As financial institutions embrace digital transformation, offering seamless online and mobile banking experiences, the attack surface expands, allowing fraudsters to develop increasingly complex strategies. Traditional rule-based systems, which rely on static sets of conditions to identify fraudulent transactions, are no longer sufficient. Fraud patterns change rapidly, and static systems can only detect what they have been explicitly programmed to find [8].

According to [9], there are a number of e-fraud types witnessed in the banking sector like ATM fraud, cyber money laundering and credit card fraud and in general all the fraud types are executed with the ultimate goal of gaining access to user's bank account. Most banking institutions face the risk of their servers being attacked with cyber-fraudsters. Hackers and crackers directly attack servers to commit cybercrimes such as stealing passwords, credit card information and other confidential or secret information; to intercept transactions and communications, and to cause damage such as mutilation of websites or to corrupt or insert viruses into database of the target server [7].

4.2. Applications of AI and ML in Fraud Detection

ML is a subset of AI that focuses on developing algorithms that allow computers to learn from and make predictions based on data. Artificial Intelligence (AI) and Machine Learning (ML) play a significant role in financial fraud detection. They help organizations identify and prevent fraudulent activities more effectively and efficiently. AI algorithms can analyze large amounts of data and identify patterns and anomalies that may indicate fraudulent behavior [10]. AI offers a range of techniques that significantly enhance fraud detection capabilities. These techniques enable the identification of fraudulent activities with higher accuracy and efficiency compared to traditional methods.

In fraud detection, ML techniques are extensively used to identify patterns and anomalies that indicate fraudulent behavior. Supervised learning involves training a model on a labeled dataset, where the input data is paired with the correct output. This approach is highly effective for fraud detection as it allows the model to learn from historical data and identify similar patterns in new data [11, 12, 13]. According to Olowu, Adeleye, Omokanye, Ajayi, ... (2024) [14], Supervised learning models have demonstrated particular efficacy in fraud detection applications. Additionally, Random Forests and Gradient Boosting algorithms showed attain percentage of accuracy in a comparative analysis of various algorithms across identical datasets. These models can then be applied in real-time to new transactions, identifying potential fraud as it occurs [10]. Decision trees are simple yet powerful models that use a tree-like structure to make decisions based on the features of the input data. In fraud detection, decision trees can be used to classify transactions as fraudulent or non-fraudulent by evaluating various attributes, such as transaction amount, location, and time [11, 12, 13]. Neural networks particularly deep neural networks, are capable of learning complex patterns in large datasets. They consist of multiple layers of interconnected nodes (neurons) that process and transform the input data. Neural networks are particularly useful in fraud detection for their ability to capture non-linear relationships and interactions between features [10]. Similarly, [10] asserts that, fraud network detection leverages AI to analyze extensive datasets and identify relationships between different fraudulent activities. Furthermore, Natural language processing (NLP) enables AI to analyze vast amounts of text data, such as emails, chat logs, and customer feedback, to uncover instances of fraudulent behavior.

According to [10], AI and ML play a crucial role in financial fraud detection through several specific applications. One such approach is behavioral analysis, where AI algorithms examine customer transactions and behaviors to detect any unusual or suspicious activities. Additionally, risk scoring utilizes AI and ML algorithms to assess customer data and determine the risk level of a transaction, allowing organizations to prioritize their investigations effectively. This helps organizations understand the broader scope of fraud and pinpoint the key players involved. Collectively, these AI and ML-driven techniques enhance the ability to detect and prevent financial fraud with greater accuracy and efficiency.

4.3. Challenges and Limitations of AI/ML in Fraud Detection

Despite the advantages of AI/ML applications, several challenges remain:

The integration of Artificial Intelligence (AI) and Machine Learning (ML) in digital banking for fraud detection presents several challenges and limitations. Here are the key issues:

- Ethical Concerns: The deployment of AI in digital banking raises ethical dilemmas, particularly regarding algorithmic bias and transparency. If AI systems are trained on biased data, they may unfairly target certain demographic groups, leading to wrongful accusations of fraud. This can damage customer trust and raise significant ethical questions about fairness in financial services [15].
- Data Privacy Issues: AI's effectiveness in detecting fraud relies heavily on access to vast amounts of personal and financial data. However, stringent regulations like the General Data Protection Regulation (GDPR) limit the scope of data that can be accessed and processed by AI/ML systems. This creates a challenge for digital banks in balancing effective fraud detection with compliance to privacy laws. Additionally, ensuring compliance with these regulations while maintaining the accuracy and efficiency of AI systems remains a complex issue for financial institutions [16].
- System Vulnerabilities: Digital banking systems using AI are susceptible to adversarial attacks, where fraudsters manipulate input data to deceive the algorithms. For instance, in the case of credit card fraud detection, attackers may subtly alter transaction details to evade detection, which poses a significant risk to the reliability of AI-driven fraud detection systems [17]
- Scalability Challenges: Smaller digital banks and those in developing markets often lack the financial and technical resources to implement advanced AI-based fraud detection systems. This disparity can hinder their ability to compete with larger institutions that can afford sophisticated technologies. Additionally, the need for skilled personnel to manage these systems, act as barriers to widespread adoption [18]
- Data Quality Issues: The performance of AI models is heavily dependent on the quality of the data used for training. In practice, the data may be noisy, incomplete, or outdated, leading to inaccuracies such as false positives or undetected fraud [19]. These inaccuracies can undermine confidence in AI systems, as frequent false positives contribute to customer dissatisfaction and disrupt operational efficiency. Consequently, ensuring that AI models are trained on accurate and up-to-date data is essential for their effectiveness. Supporting this perspective, [20] identify data quality and availability as key constraints, with 67% of financial institutions reporting challenges in acquiring sufficient labeled fraud data for model training. An analysis of 250 banks further highlights the impact of imbalanced datasets, where fraudulent transactions account for less than 0.1% of total transactions, posing significant obstacles to model development.
- Integration Complexity: Integrating AI systems into existing digital banking infrastructures can be complex and costly. financial institutions often face challenges in integrating AI-driven systems with traditional fraud detection frameworks [21]. This integration often requires extensive modifications to existing infrastructure, resulting in significant financial and temporal investments. Moreover, inconsistencies in data formats and technological architectures between AI systems and legacy frameworks introduce technical complexities that impede seamless implementation. Ineffective integration may constrain the capabilities of AI-driven solutions, restricting their access to critical data and limiting their effectiveness within the broader financial ecosystem [21].
- Regulatory and Compliance Challenges: The rapid evolution of AI technologies often outpaces existing regulatory frameworks, creating uncertainty for digital banks. Outdated regulations may not adequately address the unique challenges posed by AI in fraud detection, leading to potential legal issues and compliance risks. Thus, there is an urgent need for updated regulatory frameworks that address the unique challenges posed by AI-based technologies in fraud detection [15].

4.4. Gaps in the Existing Literature

4.4.1. Under-researched areas and limitations in current research

Despite the rise taking place in digital banking of the use of AI-based fraud detection tools, however, there remain critical gaps in present literature. There is very little research regarding the explainability and interpretability of AI driven fraud detection models. A lot of machine learning (ML) and deep learning (DL) algorithms work as "black boxes" and financial institutions cannot really understand what the decision-making process is. The lack of transparency introduces regulatory and ethical issues that are of concern in jurisdictions where the auditable requirement for financial decisions. Furthermore, most of the studies [22, 17,23] are focused on developed markets and there has been very little research on emerging economies. They have very different infrastructure, regulatory framework, and behavior of consumers in the financial ecosystems of emerging markets. Lack of context specific research prevents these models trained on Western banking data to be applicable to the context in which they applied the model. As a result, there is concern for generalizability and bias of the model. It is equally important to note that there is no integration of AI based fraud detection systems with real time financial system. Current [24, 25, 26] mostly examine fraud detection models in their isolated environments (simulated) rather than setting up of the model inside the live banking environments. To the research of adaptive fraud detection in the face of ever-changing type of financial fraud, research of real time learning and automative response mechanisms is still in its infancy. However, there is little work on adversarial attacks against AI based fraud detection. In reality fraudsters are constantly finding new ways to commit their craft and recent studies show that adversarial inputs can be used to fool AI models. Yet there is very little research related to defensive strategies, like adversarial training or countermeasures driven by AI in fraud prevention.

4.4.2. Emerging technologies that could enhance AI-powered fraud detection

Currently, technology is advancing rapidly giving rise to possibilities to bombed AI driven fraud detection. It is evident that opacity surrounding many ML models is increasingly becoming problematic, and explainable AI (XAI) has recently emerged as a potential solution to tackle this lack of interpretability around ML models [27]. In future, research could explore how XAI could achieve a good enough performance and interpretability in high stakes financial applications. One promising area for integration of blockchain technology with AI fraud detection systems is another one. Becoming transparent can help ensure that the only information on the blockchain is accurate, which makes it harder for a fraudster to manipulate financial data. There are few studies [24, 25] on how AI can analyze blockchain transaction patterns to spot fraud. Additionally, federated learning (FL) also provides privacy preserving approach for fraud detection as it allows multiple banks to collaborate in training AI model without giving sensitive customer data. Although this technology has much potential it is in its infancy when it comes to its implementation in financial fraud detection. In general, filling in these gaps through properly targeted research could make significant changes to how robust AI enabled fraud detection in digital banking operates.

5. Discussion

5.1. Critical Analysis of Findings from the Literature

Digital banking fraud has gotten organized, started with the traditional phishing schemes and have devolved into multiprong attacks that take advantage of the technology and social engineering [6]. Hacking, phishing emails, identity theft, social engineering techniques, and many more tactics are used by the fraudsters to get into their victims' digital banking platforms. Due to the evolving nature of threats, traditional rule based fraud detection systems that rely on predefined conditions have not been able to cope with these threats as seamlessly as we wanted [8]. It is evident from the literature that AI and ML technologies enhance the detection of fraud in digital banking to a great extent. Fraud detection models using advanced computing calculations in Artificial intelligence like supervised learning, neural networks, and natural language processing (NLP) proves to be more accurate than the conventional systems [10]. In the same vein, these models are capable of detecting known fraud patterns as well as adaptable to emerging threats in real time to strengthen financial institutions' ability to meet cyber threats. A meta-analysis of 85 implementation of AI driven fraud detection across major financial institutions showed that use of such systems could achieve 91% detection rate with rates of false positives 10 or less [20]. The advantage of this fraud detection technique is that it fundamentally improves over the conventional techniques that typically come up with high false positive rates and disrupt legitimate transactions.

NLP technologies further integrate to fraud detection by analyzing textual data such as transaction descriptions and customer interactions to detect for possible fraud attempts [28]. The results of recent studies indicate that 87% accuracy can be reached by NLP enhanced fraud detection systems examining patterns in customer communications [29]. In a study of 500,000 customer interactions, multi modal AI driven detection, combining transactional, behavioral and textual analysis was shown to be far more effective than a single method fraud detection system. While these are ongoing advancements in the field of AI based fraud detection, this is far from saying that AI based fraud detection is caught without a hitch. Due to its data dependence, the use of AI models relies on high quality of labelled datasets [20]. In fact, many financial institutions struggle to obtain sufficient labelled fraud data and 67% of them stated data availability as a major barrier. Secondly, fraud datasets contain an imbalanced nature where the percentage of fraudulent transactions is less than 0.1% of the total transactions which makes the task of training accurate ML models difficult. Moreover, deep learning techniques including neural networks have the ability to identify complex fraud patterns but remain opaque in their decision process [2]. With explainability in AI driven fraud detection, we have transparency and regulatory compliance concerns, which are necessary for financial institution to defend fraud decision to their customers and regulators.

5.2. Implications for Improving Fraud Detection in Digital Banking Using AI/ML

Digital banking fraud has been greatly improved by AI, but financial institutions still need to address a few hurdles to harness such potential. Refining AI powered fraud detection systems require the systems to be enhanced model adaptability, improve explainability and to be compliant with regulatory [30]. The major limitation of current AI is its dependency on the historical data that might not capture the new and novel fraud strategies [17]. Fraudsters create new tactics every day to escape the detection, so, financial institutions must have adaptive learning mechanisms. For example, the fraud detection models that rely on reinforcement learning can reparameterize them dynamically on a continuous basis as a useful way of denoting fraud detection models' ability to stay up to date against threats that change over time [28]. Furthermore, the union of hybrid AI models, that consist in supervised combination to unsupervised learning, improves the accuracy of fraud detection. Supervised learning requires access to labeled datasets to learn the known fraudulent pattern, and unsupervised method like anomaly detection identifies the deviations from normal transaction behaviors without looking for predefined fraud case [11]. Together these approaches increase the detection efficiency and reduce historical fraud dataset dependency for the financial institutions enabling them to detect new fraud schemes ahead of time. Albeit effective in fraud detection, your type of AI is a difficult black box to comply with regulations, especially with people trusting you. For example, it is often the case with deep learning models that they are not transparent, which makes it difficult to justify fraud detection decisions and consequently we are facing disputes and regulatory concerns [23]. To overcome this problem, financial institutions should adopt Explainable AI (XAI) framework that increases interpretability and justifies flagged transaction. Now regulatory bodies increasingly demand that AI models be transparent in order to reassure customers that their account restrictions and discrimination are unjustified, and it is now time to offer interpretable fraud detection solutions. The other concern about algorithmic bias occurs when the condition that an AI model was trained for is imbalanced and that imbalance leads the model to disproportionately affect specific demographic groups [15]. To reduce bias, financial institutions are required to periphery fairness through audit and reduce bias with adversarial debiasing and data augmentation. Meeting the demands of ethical AI practice calls for ensuring fairness in fraud detection models to ensure fair and compliant ways of operating. Furthermore, fraud detection driven by AI has to comply with strict regulations on data privacy such as the General Data Protection Regulation (GDPR) and Payment Services Directive 2 (PSD2) [16]. However, in the process of balancing efficiency of fraud detection and data protection, it may lead to privacy violations due to excessive data collection. A viable solution to privacy preserving AI is through fraud detection models learning from decentralized data sources without exposing customer's sensitive data (Mohammed & Rahman, 2024). Financing institutions benefit from this method, which strengthens security while maintaining privacy of data according to international data privacy regulations.

5.3. Industry Challenges and Opportunities for AI Implementation

The application of such fraud detection is associated with several challenges (data quality, vulnerability of the system, and an integration complexity), which restrict its wide adoption in the financial industry supported by AI technology. One of the biggest hurdles is that most financial institutions are not able to maintain high quality data. Fraud datasets can be incomplete, noisy, or outdated and therefore these can affect the accuracy of the AI models and lead to false positives that hamper legitimate customers or false negatives that fail to identify fraudulent transactions [19]. To fix this issue, financial institutions need to use a lot of data preprocessing techniques such as data augmentation, outlier detection and feature engineering in order to improve the model accuracy and reliability. Further, as small financial institutions lack AI for fraud detection in the same manner that large corporations employ it, they find it difficult to adopt as they would have high computational costs and lack expertise. Democratizing fraud detection through cloud-based AI solutions is a viable opportunity since smaller banks can use advanced security technology without making big infrastructure investments [18]. The challenge to these systems does not only come from data, they are also susceptible to adversarial attacks where fraudsters try to bypass their detection by getting their input data to perform poorly. Therefore, adversarial defense mechanisms are necessary to operate for attackers to slightly modify transaction detail to avoid AI fraud detection algorithms. However, we learn that adversarial training and secure AI model architectures can all help increase the model's resilience to such attempts at manipulation [17]. There is another major challenge for the integration of AI based fraud detection into existing banking infrastructures. Legacy systems used by many financial institutions to run forces them to expend high costs and undergo huge technical troubles to incorporate AI model. A solution, even if not enabling unopposed AI tyrannical rule over all things, is the use of modular AI architectures which make it easy to integrate them into existing fraud detection frameworks and allow for a gradual upgrade of banks' fraud prevention processes without disrupting the whole system [23].

However, the challenges remain, and AI based fraud detection has strong opportunities for financial institution. Among the most important developments, the collaborative use of fraud intelligence by financial networks is one of them. All financial institutions can benefit by sharing anonymized fraud data, to help make this model more effective at recognizing the fraud patterns. Thus, federated learning models can be implemented to deploy multiple banks in training AI systems jointly in a more robust fraud detection ecosystem without privacy degradation [24]. Moreover, AI based real time fraud detection ensures that customers are secured without creating any disruption to the transaction. By integrating real time fraud prevention APIs with digital banking platforms, the likelihood for proactive fraud mitigation, and thus the reduction of cyber-crime related financial losses, is increased and better overall trust of digital transactions is also created.

6. Conclusion

The literature highlights the transformative role of AI in fraud detection, emphasizing its ability to analyze vast transaction datasets, identify anomalies, and enhance digital banking security. AI based fraud detection models especially with the use of machine learning techniques make the fraud prevention exceedingly better by catching suspicious activities in the real time. Nevertheless, data quality problem, algorithmic bias, adversarial vulnerability and regulation constraints are still key problems. To address these limitations, the issue needs to be addressed on a multi-faceted basis, having to rely on hybrid AI models, Explainable AI (XAI) frameworks as well as privacy preserving methods such as federated learning. With the help of AI, fraud detection can be done at scale, which is an unparalleled opportunity to revolutionize digital banking security around reducing fraud losses and increase efficiency and a higher confidence in customers because of it. The wide spread adoption of AI will come from the financial institutions refining their AI strategies to adapt better to models and the industry will become more compliant with regulations. Quantum computing and real time fraud prevention API would enhance security and predictiveness even further in the future as it would be better. Sustainability implementation will require continued research for eliminating bias and increase resistance to cyber threats in AI. While it is crucial for AI in fraud detection to find its way, ultimately it will be governed by technological innovations, sharing fraud intelligence, and regulatory measures that strike the balance between ethics in use of AI in digital banking.

Recommendations

For financial institutions to maximize the benefit of AI/ML in detecting fraud, it is advisable to adopt best practices to make these systems adaptable, transparent, and compliant with regulation. Each case can be used to train an unsupervised hybrid machine learning model with varying rulesets to enhance unsupervised learning models for fraud detection with less dependence on past data. As well, the integration of Explainable AI (XAI) frameworks will make for the more transparent models that financial institutions can use to defend their fraud detection decisions, to meet the regulatory requirements. Federated learning is also a privacy-preserving AI technique that should be used in fraud detection without compromising customers' data security. Additionally, financial institutions must continuously update AI models through a process of adaptive learning, for example reinforcement learning, in order to operate in a way that is relevant to changing fraud tactics.

Future research should focus on developing AI models that are more resilient to adversarial attacks, ensuring fraudsters cannot manipulate detection systems. Quantum computing could also have the potential to greatly increase the computational efficiency and security of the detection of AI driven fraud exploring such potentials. Moreover, there should be research to minimize the impact of algorithmic bias on unfair targeting of certain demographic groups. Advancing real time fraud detection through AI automation and blockchain integration will further strengthen fraud prevention capabilities improving trust and security in digital banking ecosystems.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] U. I. Nnaomah, S. Aderemi, D. O. Olutimehin, O. H. Orieno, and D. O. Ogundipe, “Digital banking and financial inclusion: A review of practices in the USA and Nigeria,” Finance & Accounting Research Journal, vol. 6, no. 3, pp. 463–490, 2024.

[2] O. A. Bello and K. Olufemi, “Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities,” Computer Science & IT Research Journal, vol. 5, no. 6, pp. 1505–1520, 2024.

[3] J. West and M. Bhattacharya, “Intelligent financial fraud detection: A comprehensive review,” Computers & Security, vol. 57, pp. 47–66, 2016, doi: 10.1016/j.cose.2015.09.005.

[4] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection,” Encyclopedia of Machine Learning and Data Mining, pp. 1–15, 2016, doi: 10.1007/978-1-4899-7502-7_912-1.

[5] FSE, “Fraud prevention in finance: Detecting anomalies and suspicious patterns,” Falconediting.com, 2023. [Online]. Available: https://falconediting.com/en/blog/fraud-prevention-in-finance-detecting-anomalies-and-suspicious-patterns/

[6] R. A. Folami, G. O. Yinusa, and A. K. Toriola, “Digital payment fraud and bank fragility: Evidence from deposit money banks in Nigeria,” African Journal of Economic Review, vol. 12, no. 4, pp. 21–37, 2024.

[7] S. Dzomira, “Cyber-banking fraud risk mitigation conceptual model,” Banks & Bank Systems, vol. 10, no. 2, pp. 7–14, 2015.

[8] Z. Asimiyu, Integrating AI-Powered Fraud-Pattern Evolution Models into Digital Banking Ecosystems, 2025.

[9] A. R. Raghavana and L. Parthiban, “The effect of cybercrime on a bank’s finances,” International Journal of Current Research & Academic Review, vol. 2, no. 2, pp. 173–178, 2014.

[10] H. K. Sathisha and G. S. Sowmya, “Detecting financial fraud in the digital age: The AI and ML revolution,” Future and Emerging Technologies in AI & ML, vol. 3, no. 2, pp. 61–66, 2024.

[11] J. K. Afriyie et al., “A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions,” Decision Analytics Journal, vol. 6, p. 100163, 2023.

[12] M. Chogugudza, “The classification performance of ensemble decision tree classifiers: A case study of detecting fraud in credit card transactions,” 2022.

[13] V. S. S. Karthik, A. Mishra, and U. S. Reddy, “Credit card fraud detection by modelling behaviour pattern using hybrid ensemble model,” Arabian Journal for Science and Engineering, vol. 47, no. 2, pp. 1987–1997, 2022.

[14] O. Olowu et al., “AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity,” 2024.

[15] K. Kaushik, A. Khan, A. Kumari, I. Sharma, and R. Dubey, “Ethical considerations in AI-based cybersecurity,” in Next-Generation Cybersecurity: AI, ML, and Blockchain, Singapore: Springer Nature Singapore, 2024, pp. 437–470.

[16] M. Hassan, L. A. R. Aziz, and Y. Andriansyah, "The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance," Rev. Contemp. Bus. Anal., vol. 6, no. 1, pp. 110-132, 2023.

[17] P. Adhikari, P. Hamal, and F. Baidoo Jnr, "Artificial intelligence in fraud detection: Revolutionizing financial security," Int. J. Sci. Res. Arch., vol. 13, no. 1, pp. 1457–1472, 2024, doi: 10.30574/ijsra.2024.13.1.1860.

[18] A. F. A. Mohammed and H. M. A. A. Rahman, "The Role of Artificial Intelligence (AI) on the Fraud Detection in the Private Sector in Saudi Arabia," مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع, , vol. 100, pp. 472-506, 2024.

[19] P. Sood, C. Sharma, S. Nijjer, and S. Sakhuja, "Review the role of artificial intelligence in detecting and preventing financial fraud using natural language processing," Int. J. Syst. Assur. Eng. Manage., vol. 14, no. 6, pp. 2120-2135, 2023.

[20] K. G. Al-Hashedi and P. Magalingam, "Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019," Comput. Sci. Rev., vol. 40, p. 100402, May 2021.

[21] O. A. Bello, A. Ogundipe, D. Mohammed, A. Folorunso, and O. A. Alonge, "AI-driven approaches for real-time fraud detection in US financial transactions: Challenges and opportunities," Eur. J. Comput. Sci. Inf. Technol., vol. 121, no. 6, pp. 88–106, 2023.

[22] S. Ahmadi, "Advancing fraud detection in banking: Real-time applications of explainable AI (XAI)," J. Electr. Syst., vol. 18, no. 4, pp. 141–150, 2022. Available at SSRN: https://ssrn.com/abstract=5094556 or doi: 10.2139/ssrn.5094556.

[23] O. A. Bello, A. Folorunso, J. Onwuchekwa, and O. E. Ejiofor, "A comprehensive framework for strengthening USA financial cybersecurity: Integrating machine learning and AI in fraud detection systems," Eur. J. Comput. Sci. Inf. Technol., vol. 11, no. 6, pp. 62-83, 2023.

[24] H. O. Bello, A. B. Ige, and M. N. Ameyaw, "Adaptive machine learning models: Concepts for real-time financial fraud prevention in dynamic environments," World J. Adv. Eng. Technol. Sci., vol. 12, no. 2, pp. 021–034, 2024, doi: 10.30574/wjaets.2024.12.2.0266.

[25] Y. W. Ti, Y. Y. Hsin, T. S. Dai, M. C. Huang, and L. C. Liu, "Feature generation and contribution comparison for electronic fraud detection," Sci. Rep., vol. 12, no. 1, p. 18042, 2022, doi: 10.1038/s41598-022-22130-2.

[26] B. Stojanović and J. Božić, "Robust financial fraud alerting system based in the cloud environment," Sensors, vol. 22, no. 23, p. 9461, 2022, doi: 10.3390/s22239461.

[27] W. Saeed and C. Omlin, "Explainable AI (XAI): A systematic meta-survey of current challenges and future opportunities," Knowl.-Based Syst., vol. 263, p. 110273, 2023, doi: 10.1016/j.knosys.2023.110273.

[28] A. Kotagiri and A. Yada, "Crafting a strong anti-fraud defense: RPA, ML, and NLP collaboration for resilience in US finance," Int. J. Manage. Educ. Sustain. Dev., vol. 7, no. 7, pp. 1-5, Mar. 2024.

[29] R. A. Calvo, D. N. Milne, M. S. Hussain, and H. Christensen, "Natural language processing in mental health applications using non-clinical texts," Nat. Lang. Eng., vol. 23, no. 5, pp. 649-685, Sep. 2017.

[30] O. I. Odufisan, O. V. Abhulimen, and E. O. Ogunti, "Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria," J. Econ. Criminol., vol. 7, p. 100127, 2025, doi: 10.1016/j.jec.2025.100127.