International Journal of Scientific Research in Modern Science and Technology
ISSN: 2583 -7605 (Online)
© IJSRMST | Vol. 4 | Issue 7 | July 2025
Available online at: https://ijsrmst.com/
DOI: https://doi.org/10.59828/ijsrmst.v4i7.345

AI-powered fraud detection in online banking: Using machine learning to improve security

N. Sugumar Babu[1] & Dr. M. Kotteeswaran[2]

[1]Research Scholar, School of Management Studies, Vels Institute of Science, Technology and Advanced Studies, (VISTAS), Chennai-600117

[2]Corresponding Author, Associate Professor, School of Management Studies, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, Chennai-600117.

[1]**Email: sugumarbabu7@gmail.com**

ABSTRACT

This study looks at how machine learning (ML) and artificial intelligence (AI) might improve fraud detection in the online banking industry. Fraudsters are growing more skilled as more financial transactions shift to digital platforms, making the implementation of advanced security measures necessary. Machine learning models that analyze large datasets, detect anomalies, and lower the risk of financial fraud are used to assist AI-driven fraud detection systems. The author of this literature study critically assesses current AI/ML-based fraud detection techniques in terms of their efficacy, difficulties they confront, and potential pathways for scaling up their use as a solution. The paper highlights important developments in deep learning models, supervised and unsupervised learning, and anomaly detection methodology. The results demonstrate AI's potential to improve fraud detection accuracy while addressing algorithmic bias, data privacy, and adversarial assault. The study concludes by offering suggestions for improving the fraud detection system with regard to real-time fraud monitoring, Explainable AI (XAI), and incorporating blockchain technology into the security of digital banking.

Keywords: *Machine learning, anomaly detection, cybersecurity, explainable AI (XAI), and AI-powered fraud detection*

1. Introduction

In times of altered financial services delivery logistics, digital banking is essential to the financial industry's development as a source of allowing financial inclusion. The revolution depends on the democratization of banking services, which have made banking faster, easier, and more convenient than before thanks to internet banking. Digital banking has a significant impact since it has the ability to integrate the underserved, unbanked, and excluded into the official financial ecosystem in addition to improving service delivery. It is obvious that the quick development of digital banking has fundamentally changed and simplified financial services. However, the risk of cybercrime has also grown to the point where organizations and customers can sustain large losses in terms of money and reputation. Concerns about cybersecurity, digital literacy, and the requirement for a robust regulatory framework are the main obstacles to making the most of the benefits of digital banking. To lessen these difficulties, machine learning can significantly improve user data and fraud detection security [1]. Generally speaking, conventional fraud detection systems (such as preset rules and historical data) are not as advanced to cover the variety of scams that are perpetrated against them. Traditional manual detection techniques are costly, time-consuming, and imprecise; they are also unworkable in the era of big data. However, due to the intricacy of the issue, these methods—which primarily use manual auditing techniques—can be unreliable and ineffective. However, the advantages of machine learning-based security enhancement are far greater because these advanced techniques can undoubtedly evaluate enormous data sets and find patterns that manual approaches could miss. Olufemi and Bello (2024) [2] thought that since AI can examine enormous volumes of data, spot trends, and reliably forecast fraudulent activities, it can provide innovative answers to this expanding issue. Data mining-based techniques have been particularly helpful since they can identify minute abnormalities in large amounts of data, improving the precision and efficacy of fraud detection [3]. As a result, AI and ML technologies have been integrated, and proactive and flexible methods for identifying fraudulent activity have been developed. The study task is predicated on a survey of the literature about the potential of AI/ML techniques to enhance digital banking fraud detection.

2. Methodology

The present practice and results of using AI-powered fraud detection in digital banking are critically reviewed and compared in this systematic review using a thorough methodological approach. Evaluating how machine learning (ML) technologies enhance security and lower fraud risks on digital banking systems is the primary goal. To give a thorough yet objective perspective of what has been reported in the literature, this review describes the data sourcing, search technique, and research selection criteria. Peer-reviewed journal publications served as the primary data sources for this review. Several academic databases, including Google Scholar, IEEE Xplore, ScienceDirect, and SpringerLink, were thoroughly searched. Keywords like AI fraud detection, machine learning in digital banking, financial institution cybersecurity, fraud protection technologies, and AI-based transaction monitoring were used in the search. Reviews were limited to English-language publications published between 2010 and the present in order to gather latest developments in AI and ML applications to detect fraud. The research was chosen based on its relevance to the review's goals, methodological rigor, and the development of our knowledge regarding how the application of AI and ML technologies improves fraud detection in digital banking. The inclusion criteria were empirical research, theoretical frameworks, technical case studies, and industry reports that explore the ways in which artificial intelligence (AI) might improve the efficacy, difficulties, and practical application of fraud detection systems. However, research that was deemed insufficiently rigorous or unrelated to AI-based fraud detection was excluded based on exclusion criteria. In order to give the reader a thorough and knowledgeable understanding of how AI and machine learning technologies are transforming fraud detection in digital banking, the review adheres to this methodical approach. In order to help financial institutions, regulatory agencies, and technology developers safeguard their digital finances and combat fraud in the emerging digital finance space, the findings are intended to offer valuable insights.

3. Theoretical Framework

3.1. Theory of Anomaly Detection:

One fundamental method for identifying fraudulent transactions is the Anomaly Detection Theory, which looks for odd patterns or behavior that differs from the norm [4]. Anomalies in the realm of digital banking, such as irregular transaction volumes, strange login locations, abrupt shifts in spending patterns, or unexpected account activity patterns, are frequently fraudulent operations [5]. By locating transaction data outliers that deviate from expected behavior, anomaly detection is utilized in digital banking to identify new fraudulent schemes, according to [2]. This theory addresses the fundamental issue of separating these anomalies from large datasets and assists financial institutions in proactively identifying possible frauds before serious harm is done. Numerous fields, including credit card fraud detection, insurance claims analysis, healthcare monitoring, and cybersecurity intrusion detection, have made extensive use of anomaly detection [4]. Banks can reduce false positives and increase the likelihood of identifying actual fraudulent activity by integrating anomaly detection into their fraud prevention systems.

3.2. Decision Framework for Machine Learning:

Artificial intelligence (AI) methods including machine learning (ML), deep learning, and natural language processing (NLP) have completely changed the identification and prevention of fraud. Using machine learning methods, supervised learning models like decision trees and neural networks are frequently employed to identify these fraudulent transactions based on previous data. The help of these models, it will be feasible to differentiate between legitimate and fraudulent transactions because the latter may be distinguished from billiard by identifying minute patterns that are difficult for basic systems with rules. According to [2], because deep learning, a subset of machine learning, can process and analyze unstructured data like text, audio, or images, it has shown great promise in the identification of fraud. CNNs and RNNs are utilized in applications such as credit card fraud detection and anti-money laundering (AML) to achieve methods. By analyzing textual data, such as emails and transaction descriptions that have been recorded, language processing helps identify fraudulent behavior by identifying patterns and suspect language. Fraud prevention is much more than just detection; it also includes preventive steps that use artificial intelligence. AI helps businesses anticipate potential fraud hotspots so they can put preventative measures in place to stop the crime from happening. Real-time monitoring systems that use AI provide immediate alerts on questionable activity, allowing for quick action to combat fraud. These frameworks offer a starting point for comprehending how AI and ML technologies improve digital banking's ability to detect fraud.

4. Literature Review

4.1. Online Banking Fraud

Digital banking fraud, a more general term that includes online banking, refers to fraudulent activity on a range of digital financial platforms, such as digital payment systems, online banking, and mobile banking [6]. Targeting consumers of online banking as well as other digital financial services, fraudsters may use a variety of strategies, including hacking, phishing emails or websites, unprotected logins, website cloning, or data theft. Financial services organizations, which are frequently the targets of cybercriminals, are subject to a variety of malware assaults, including identity theft, keystroke logging, and online phishing, according to [7].From straightforward phishing scams to complex, multi-layered attacks that take advantage of cutting-edge technologies and social engineering strategies, fraud in digital banking has changed over time. As financial institutions embrace digital transformation and offer seamless online and mobile banking experiences, the attack surface expands, giving criminals the opportunity to develop ever-more-complex strategies... Conventional rule-based systems are no longer adequate for detecting fraudulent transactions since they depend on static sets of criteria. Static systems can only identify what they have been specifically designed to locate, and fraud patterns are subject to quick changes [8].

[9] claims that a variety of e-fraud kinds, including credit card fraud, ATM fraud, and cyber money laundering, are observed in the banking industry. Generally speaking, the ultimate objective of all fraud types is to obtain access to the victim's bank account. The majority of financial organizations run the danger of having cybercriminals assault their servers. Hackers and crackers target servers directly in order to carry out cybercrimes like password theft, credit card fraud, and other secret or confidential data theft; intercept communications and transactions; and cause harm like website tampering or virus insertion into the target server's database [7].

4.2. AI and ML Applications for Fraud Detection

The goal of machine learning (ML), a branch of artificial intelligence, is to create algorithms that let computers analyze data and draw conclusions. The identification of financial fraud is greatly aided by machine learning (ML) and artificial intelligence (AI). They facilitate more effective and efficient fraud detection and prevention for enterprises. Large data sets may be analyzed by AI systems, which can then spot trends and abnormalities that might point to fraud [10].AI provides a number of methods that greatly improve the ability to detect fraud. Compared to conventional procedures, these strategies allow for the more accurate and efficient identification of fraudulent operations.

Machine learning algorithms are widely utilized in fraud detection to find trends and abnormalities that point to fraudulent activity. Training a model on a labeled dataset—where the input data is coupled with the appropriate output—is known as supervised learning. Because it enables the model to learn from past data and spot comparable patterns in fresh data, this method is quite successful at detecting fraud [11, 12, 13]. Olowu, Adeleye, Omokanye, Ajayi, … (2024)[14] state that supervised learning models have been very effective in situations involving fraud detection. Additionally, in a comparison analysis of different algorithms across identical datasets, Random Forests and Gradient Boosting techniques demonstrated an increasing proportion of accuracy. These models can then be used to detect possible fraud as it happens by applying them in real-time to fresh transactions [10]. Decision trees are simple yet powerful models that use a tree-like structure to base their decisions on the properties of the incoming data. By analyzing multiple factors, including transaction amount, location, and time, decision trees can be utilized in fraud detection to categorize transactions as either fraudulent or non-fraudulent [11, 12, 13]. Neural networks, particularly deep neural networks, are capable of learning complex patterns in large datasets. The input data is processed and transformed by their several layers of interconnected nodes, or neurons. Because neural networks can capture non-linear correlations and interactions between features, they are especially helpful in fraud detection [10]. In a similar vein, [10] claims that fraud network identification uses AI to examine large datasets and find connections between various fraudulent behaviors. Additionally, AI can examine enormous volumes of text data, like emails, chat logs, and customer reviews, thanks to natural language processing (NLP), which helps identify instances of fraudulent activity.

Through a number of specialized applications, AI and ML are essential in the detection of financial crime, according to [10]. Behavioral analysis is one such method, in which AI systems look at consumer transactions and actions to identify any anomalous or dubious actions. Furthermore, risk scoring enables businesses to efficiently prioritize their investigations by evaluating consumer data and estimating the risk level of a transaction using AI and ML algorithms. This aids businesses in identifying the main participants and comprehending the fraud's wider scale. When combined, these AI and ML-driven methods improve the precision and effectiveness of financial fraud detection and prevention.

4.3. AI/ML's Difficulties and Limitations in Fraud Detection

Even with the benefits of AI/ML applications, there are still a number of obstacles to overcome:

There are a number of difficulties and restrictions when integrating machine learning (ML) and artificial intelligence (AI) in digital banking for fraud detection. These are the main problems:

Ethical Issues: Using AI in digital banking presents ethical issues, especially with relation to algorithmic bias and transparency. AI systems may unjustly target particular demographic groups if they are trained on biased data, which could result in false fraud accusations. This has the potential to undermine consumer confidence and bring up important moral dilemmas regarding equity in financial services [15].

Data privacy concerns: AI's ability to identify fraud is largely dependent on its ability to access enormous volumes of financial and personal data. However, the range of data that AI/ML systems can access, and handle is constrained by strict laws like the General Data Protection Regulation (GDPR). This makes it difficult for online banks to strike a balance between adhering to privacy regulations and effectively detecting fraud. Furthermore, it is still difficult for financial institutions to ensure compliance with these requirements while preserving the precision and effectiveness of AI systems [16].

System Vulnerabilities: Adversarial attacks, in which scammers alter input data to trick algorithms, can affect AI-powered digital banking systems. The dependability of AI-driven fraud detection systems is seriously jeopardized in the case of credit card fraud detection, for example, where attackers may covertly change transaction information to avoid detection [17].

Scalability Issues: Digital banks in developing nations and smaller ones frequently lack the financial and technical means to deploy sophisticated AI-based fraud detection systems. This difference may make it more difficult for them to the capacity to contend with bigger organizations that can afford more advanced technology. Widespread adoption is further hampered by the requirement for qualified staff to administer these systems [18].

Data Quality Issues: The caliber of the training data has a significant impact on how well AI models work. In actuality, the data could be noisy, lacking, or out-of-date, which could result in errors like false positives or fraud that goes unnoticed [19]. Because frequent false positives result in unhappy customers and reduce operational efficiency, these errors have the potential to erode trust in AI systems. Therefore, it is crucial for AI models to be trained on current and accurate data in order for them to be effective. According to [20], which supports this viewpoint, 67% of financial institutions report difficulties obtaining enough labeled fraud data for model training, making data availability and quality the primary bottleneck. The significance of imbalanced datasets, where fraudulent transactions make up less than 0.1% of total transactions, is further highlighted by an investigation of 250 institutions, which presents major challenges for model building.

Complexity of Integration: It might be difficult and expensive to integrate AI technologies into current digital banking infrastructures. Integrating AI-driven technologies with conventional fraud detection frameworks is frequently difficult for financial institutions [21]. This integration frequently necessitates major changes to the current infrastructure, which calls for large time and expense commitments. Furthermore, technical complications that prevent smooth deployment are introduced by differences in data formats and technological structures between AI systems and traditional frameworks. AI-driven solutions' potential may be limited by inefficient integration, which would also limit their efficacy in the larger financial ecosystem by limiting their access to vital data [21].

Regulatory and Compliance Issues: Digital banks face ambiguity as a result of the quick development of AI technologies, which frequently surpasses the current regulatory frameworks. The special difficulties presented by AI in fraud detection may not be sufficiently addressed by outdated legislation, which could result in legal problems and compliance risks. Therefore, new regulatory frameworks that take into account the particular difficulties presented by AI-based solutions in fraud detection are desperately needed [15].

4.4. The Existing Literature's Gaps

4.4.1. Limitations and understudied areas in the present research

However, there are still significant gaps in the current literature despite the growing usage of AI-based fraud detection systems in digital banking. Research on the interpretability and explainability of AI-driven fraud detection models is extremely limited. Many deep learning (DL) and machine learning (ML) algorithms operate as "black boxes," and financial institutions are unable to fully comprehend the decision-making process. In jurisdictions where financial choices must be auditable, the absence of transparency raises ethical and regulatory concerns. Additionally, there has been relatively little research on emerging economies, with the majority of studies [22, 17, 23] concentrating on developed markets. The regulatory environment, consumer behavior, and infrastructure of emerging market financial ecosystems varied greatly. These models trained on context-specific data are unable to data from Western banks to be relevant to the situation where they used the model. Consequently, the model's bias and generalizability are questioned. It's also crucial to remember that real-time financial systems and AI-based fraud detection systems are not integrated. Instead of configuring the model in real-world banking settings, current [24, 25, 26] primarily study fraud detection models in their isolated contexts (simulated). Research on real-time learning and automated reaction mechanisms is still in its early stages when it comes to adaptive fraud detection in the face of constantly evolving financial fraud types. Adversarial assaults against AI-based fraud detection, however, have not received much attention. In actuality, scammers are always coming up with new ways to commit their crimes, and new research indicates that adversarial inputs can be utilized to trick AI algorithms. However, there is a dearth of research on defensive tactics, such as AI-powered countermeasures or adversarial training, in the fight against fraud.

4.4.2. New technology that could improve fraud detection using AI

At the moment, technology is developing quickly, opening the door to the possibility of AI-driven fraud detection. It is clear that the opacity around many machine learning models is becoming a bigger issue, and explainable artificial intelligence (XAI) has lately surfaced as a possible remedy to address this interpretability issue [27]. Future studies could examine how XAI might perform and interpret well enough in high-stakes financial applications. Another area that shows promise for blockchain technology integration with AI fraud detection systems is this one. Transparency can help guarantee that the blockchain contains only accurate information, making it more difficult for fraudsters to alter financial data. Studies on AI's ability to identify fraud by analyzing blockchain transaction patterns are scarce [24, 25]. Federated learning (FL), which enables several banks to work together to build AI models without disclosing private client information, also offers a privacy-preserving method for fraud detection. Even though this technology has a lot of promise, its use in the detection of financial crime is still in its infancy. Generally speaking, closing these gaps with carefully focused research could have a big impact on how reliable AI-enabled fraud detection in online banking functions.

5. Discussion

5.1. Evaluation of Literature Results Critically

The organized fraud in digital banking began with classic phishing attempts and grew into multifaceted attacks that exploit social engineering and technology [6]. Identity theft, phishing emails, social engineering, hacking, and many other strategies are employed by scammers to get access to their victims' online banking accounts. Traditional rule-based fraud detection systems that depend on predetermined criteria have not been able to handle these threats as smoothly as we would have liked because of their dynamic nature [8]. The literature makes it clear that AI and ML technologies significantly improve the detection of fraud in online banking. Fraud detection algorithms that employ sophisticated artificial intelligence computations, such as neural networks, supervised learning, and natural language processing (NLP), outperform traditional systems in terms of accuracy [10]. Similarly, these models can both identify established fraud trends and instantly adjust to new threats, enhancing financial institutions' defenses against online attacks. According to a meta-analysis of 85 AI-driven fraud detection implementations from large financial institutions, using such systems might result in a 91% detection rate with false positive rates of 10 or lower [20]. This fraud detection method has the advantage of being a significant improvement over traditional methods, which frequently produce large false positive rates and interfere with valid transactions.

By examining textual data, including transaction descriptions and customer interactions, NLP technology further integrates with fraud detection by looking for potential fraud attempts [28]. According to current research, NLP-enhanced fraud detection systems that look for patterns in consumer conversations can achieve an accuracy of 87% [29]. 500,000 consumer interactions were studied using multimodal AI-driven detection that combined transactional and behavioral, and it was demonstrated that textual analysis was considerably more successful than a fraud detection system that only used one strategy. Even while there have been continuous developments in the field of AI-based fraud detection, this does not imply that it is flawless. The usage of AI models depends on high-quality labelled datasets because of its data reliance [20]. Actually, getting enough tagged fraud data is a challenge for many financial institutions, and 67% of them cited data availability as a key obstacle. Second, the challenge of training correct machine learning models is challenging due to the imbalanced nature of fraud datasets, where the proportion of fraudulent transactions is less than 0.1% of all transactions. Since nt transactions make up fewer than 0.1% of all transactions, it is challenging to develop precise machine learning models. Furthermore, while deep learning methods like neural networks may recognize intricate fraud patterns, their decision-making process is opaque [2]. In order for financial institutions to defend their fraud decisions to their clients and regulators, explainability in AI-driven fraud detection raises issues with transparency and regulatory compliance.

5.2. Consequences for Using AI/ML to Improve Fraud Detection in Digital Banking

AI has significantly reduced digital banking fraud, but financial institutions still need to overcome a few obstacles before they can fully utilize this potential. Enhancing model adaptability, explainability, and regulatory compliance are all necessary for improving AI-powered fraud detection systems [30]. Current AI's primary drawback is its reliance on previous data, which may not account for fresh and innovative fraud tactics [17]. Financial institutions need to have adaptive learning systems since fraudsters come up with new strategies every day to avoid detection. For instance, the ability of fraud detection models that use reinforcement learning to continuously and dynamically reparameterize themselves is a helpful indicator of the models' capacity to remain current with evolving risks [28]. Additionally, the accuracy of fraud detection is increased by combining hybrid AI models, which combine supervised and unsupervised learning. While unsupervised techniques like anomaly detection find deviations from typical transaction behaviors without searching for preset fraud cases, supervised learning needs access to labeled datasets in order to learn the known fraudulent pattern [11].. When combined, these strategies improve detection effectiveness and lessen reliance on existing fraud datasets, allowing financial institutions to identify emerging fraud schemes early. Even though your kind of AI is good at detecting fraud, it is a challenging black box to comply with regulations, especially when people are putting their trust in you. For instance, deep learning models frequently lack transparency, which makes it challenging to defend fraud detection judgments. As a result, we are dealing with disagreements and regulatory issues [23]. Financial institutions could use the Explainable AI (XAI) architecture, which improves interpretability and explains flagged transactions, to solve this issue. It's time to provide interpretable fraud detection solutions since regulatory authorities are now requiring AI models to be transparent in order to persuade consumers that their discrimination and account limitations are unwarranted. The second issue with algorithmic bias arises when an AI model is trained under an unbalanced scenario, which causes the model to disproportionately impact particular demographic groups [15]. Financial organizations must use auditing to ensure fairness on the perimeter and adversarial debiasing and data augmentation to lessen bias. Ensuring fairness in fraud detection models is necessary to meet the requirements of ethical AI practice and guarantee equitable and legal methods of operation. Additionally, AI-powered fraud detection must abide by stringent data protection laws like the Payment Services Directive 2 (PSD2) and the General Data Protection Regulation (GDPR) [16]. However, the process of striking a balance between data protection and fraud detection effectiveness could result in privacy violations because of over-collection of data. Fraud detection models that learn from decentralized data sources without disclosing sensitive consumer information are a workable option to privacy-preserving AI (Mohammed & Rahman, 2024). This approach benefits financial organizations by enhancing security and protecting data privacy in accordance with global data privacy laws.

5.3. Industry Difficulties and AI Implementation Opportunities

The implementation of such fraud detection is hampered by a number of issues (data quality, system vulnerability, and integration complexity), which limit its widespread use in the AI-supported financial sector.One of the main challenges is that most financial institutions are unable to maintain high-quality data. The accuracy of AI models can be impacted by fraud datasets that are noisy, out-of-date, or missing. This can result in false negatives that miss fraudulent transactions or false positives that hinder real consumers [19]. Financial organizations must employ a variety of data preprocessing methods, including feature engineering, data augmentation, and outlier detection, to address this problem and raise the accuracy and dependability of the model. Furthermore, small financial institutions find it challenging to use AI since they lack the necessary expertise and incur substantial computing expenses to detect fraud in the same way that major firms do. Since smaller banks can leverage cutting-edge security technology without having to make significant infrastructure investments, democratizing fraud detection with cloud-based AI solutions is a feasible potential [18]. These systems face challenges from data alone, but they are also vulnerable to adversarial attacks, in which scammers attempt to evade detection by making their input data perform poorly. As a result, in order for attackers to circumvent AI fraud detection algorithms, adversarial defense measures must be in place. Nevertheless, we discover that safe AI models and adversarial training architectures can all contribute to making the model more resistant to these kinds of manipulation attempts [17]. The incorporation of AI-based fraud detection into current banking infrastructures faces yet another significant obstacle. Many financial organizations must incur significant expenses and deal with significant technical challenges in order to integrate AI models into their legacy systems. Even if it doesn't allow for unchecked AI tyrannical control over everything, using modular AI architectures is a solution because they are simple to incorporate into pre-existing fraud detection frameworks and enable a gradual improvement of banks' fraud prevention procedures without causing systemic disruptions [23].

Financial institutions stand to benefit substantially from AI-based fraud detection, but there are still challenges to be solved. The cooperative use of fraud intelligence by financial networks is one of the most significant advances. Everybody Financial institutions can increase the efficacy of this methodology in identifying fraud patterns by exchanging anonymized fraud data. In order to train AI systems collaboratively across several institutions in a more resilient fraud detection ecosystem without compromising privacy, federated learning models can be used [24].Furthermore, real-time fraud detection powered by AI guarantees that clients are protected without interfering with the transaction.Real-time fraud prevention APIs can be integrated with digital banking platforms to improve general trust in digital transactions and raise the possibility of proactive fraud mitigation, which lowers financial losses associated with cybercrime.

6. Conclusion

The literature emphasizes how artificial intelligence (AI) is revolutionizing fraud detection by analyzing large transaction databases, spotting irregularities, and boosting the security of digital banking. By identifying questionable activity in real time, AI-based fraud detection algorithms, particularly when combined with machine learning approaches, greatly improve fraud protection. Nevertheless, data quality problem, algorithmic bias, adversarial vulnerability and regulation constraints are still key problems. In order to overcome these constraints, a comprehensive approach is required, utilizing Explainable AI (XAI) frameworks, hybrid AI models, and privacy-preserving techniques like federated learning.Large-scale fraud detection is made possible by AI, which presents an unmatched chance to transform digital banking security by lowering fraud losses and boosting productivity and customer confidence. As financial institutions improve their AI strategies to better fit models and the industry becomes more regulatorily compliant, AI will be widely adopted. In the future, security and predictiveness would be further improved by quantum computing and real-time fraud prevention APIs. Implementing sustainability will necessitate ongoing research to eradicate bias and strengthen AI's defenses against cyberattacks. Even while AI in fraud detection is essential, in the end, it will be controlled by technological advancements, the exchange of fraud intelligence, and laws that balance ethics in the application of AI in online banking.

Recommendations

Financial institutions should use best practices to make these systems flexible, transparent, and regulatory-compliant in order to optimize the use of AI/ML in fraud detection. To improve unsupervised learning models for fraud detection with less reliance on historical data, each instance can be used to train an unsupervised hybrid machine learning model with different rulesets. In order to comply with regulatory obligations, financial institutions will also be able to justify their fraud detection judgments using more transparent models created by the integration of Explainable AI (XAI) frameworks. Federated learning is another AI method that protects privacy and ought to be applied to fraud detection without jeopardizing the security of consumer data. Additionally, in order to function in a manner that is pertinent to evolving fraud strategies, financial institutions must constantly update AI models through a process of adaptive learning, such as reinforcement learning.In order to prevent fraudsters from manipulating detection systems, future research should concentrate on creating AI models that are more resistant to adversarial attacks. Investigating such possibilities, quantum computing may also significantly improve the computational security and efficiency of AI-driven fraud detection. Additionally, studies should be conducted to lessen the effect of algorithmic bias on the unjust targeting of particular demographic groups.Enhancing real-time fraud detection via blockchain integration and AI automation will fortify fraud prevention capabilities and boost security and trust in digital banking ecosystems.

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-andsuspicious-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 واألدب وعلوم اإلنسانيات واالجتماع, , 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.

Cite this Article:

N. Sugumar Babu & Dr. M. Kotteeswaran, "AI-powered fraud detection in online banking: Using machine learning to improve security", *International Journal of Scientific Research in Modern Science and Technology (IJSRMST), ISSN: 2583-7605 (Online), Volume 4, Issue 7, pp. 01-13, July 2025.*

Journal URL: *https://ijsrmst.com/*

DOI: *https://doi.org/10.59828/ijsrmst.v4i7.345*.