International Journal of
Finance
(IJF)

The Role of Artificial Intelligence and Robotic Process Automation (RPA) in Fraud Detection: Enhancing Financial Security through Automation

CARI Journals

International Journal of Finance

ISSN 2520-0852 (Online)

Vol. 10, Issue No. 3, pp. 80 - 100, 2025 www.carijournals.org

The Role of Artificial Intelligence and Robotic Process Automation (RPA) in Fraud Detection: Enhancing Financial Security through Automation

Faith Onyemowo Godwin

Ahmadu Bello University Zaria, Nigeria,

https://orcid.org/0009-0006-5093-7442

Accepted: 26th Feb, 2025, Received in Revised Form: 26th Mar, 2025, Published: 26th Apr, 2025

Abstract

Purpose: The growing sophistication of financial fraud in the banking sector has necessitated the adoption of advanced technical solutions such as artificial intelligence (AI) and robotic process automation (RPA) to enhance fraud detection and prevention. This study examines the role, effectiveness, and challenges of AI and RPA in combating financial fraud, addressing gaps left by traditional rule-based systems.

Methodology: This study employs a literature review methodology, synthesizing existing research, case studies, and industry reports to evaluate the impact of AI and RPA on fraud detection. Key themes analyzed include real-time analytics, anomaly detection, predictive modeling, operational efficiency, and implementation challenges.

Findings: The findings reveal that AI significantly improves fraud detection accuracy, reduces false positives, and adapts to emerging threats, while RPA enhances compliance and operational efficiency by automating repetitive tasks. However, challenges such as algorithmic bias, adversarial AI attacks, data privacy concerns, high implementation costs, and ethical dilemmas around transparency and accountability hinder widespread adoption. Despite these obstacles, financial institutions report substantial reductions in fraud-related losses after integrating AI and RPA.

Unique contribution to theory, practice and policy (recommendations): This study contributes to theory by consolidating insights on AI and RPA's transformative potential in fraud detection. For practice, it recommends investing in explainable AI, robust adversarial defense mechanisms, and cost-effective RPA integration. Policymakers should establish ethical AI governance frameworks, promote regulatory alignment, and incentivize innovation to ensure financial security and transparency. The study underscores that maximizing the benefits of AI and RPA requires continuous technological advancement, ethical oversight, and collaborative regulatory efforts.

Keywords: *Fraud Detection, Artificial Intelligence (AI), Robotic Process Automation (RPA, Financial Security, Machine Learning*

1 Background to the Study

Technological advancements have persistently occupied a central role in initiatives aimed at mitigating fraudulent activities, transitioning from rudimentary rule-based frameworks to increasingly elaborate and adaptive solutions that capitalize on modern innovations. Conventional fraud detection methodologies, despite exhibiting a degree of efficacy, often fail to adequately recognize complex and evolving fraudulent operations, thereby necessitating the creation of enhanced instruments that substantially elevate the accuracy and effectiveness of detection efforts (Al-Hashedi & Magalingam, 2021; Dhieb et al., 2020; Hilal, Gadsden, & Yawney, 2022). Given that financial fraud within the banking industry encompasses a diverse array of illicit activities, the swift advancement of technology has reconfigured the landscape of threats. Recent research suggests that perpetrators of fraud are increasingly utilizing automation and artificial intelligence (AI) to execute intricate, multi-faceted attacks, a transition that demands correspondingly advanced detection and prevention mechanisms (Kartheek & Bala, 2023; Sharma, Mehta, & Sharma, 2024).

The quick digitization of banking services and increasingly complex cybercriminal strategies has led to a rise in fraudulent activity in the worldwide financial sector. The Association of Certified Fraud Examiners (2022) estimates that fraud costs financial institutions 5% of their yearly income, with banking fraud alone costing over $40 billion worldwide in 2021. Regional instances further illuminate the seriousness of the matter; for example, in Nigeria, 24 commercial banks incurred losses amounting to N5.79 billion due to fraud in Q2 2023, a dramatic increase compared to Q1 losses, and fraudulent loans represented nearly 94.35% of these losses, with additional difficulties arising from computer and mobile fraud (Akintaro, 2023). Globally, forecasts predict that financial detriments resulting from fraud will increase by 14%, escalating from $44.3 billion in 2024 to $107 billion by 2029, with the growth of e-commerce markets further amplifying opportunities for fraudsters (Adewumi, 2024; Oloni, 2024). The number and complexity of contemporary financial crimes are too great for traditional fraud detection techniques like rule-based systems and manual transaction evaluations (Deloitte, 2021). These technologies frequently produce significant false-positive rates, which strain operational resources and postpone the discovery of real threats. In order to improve detection accuracy, speed up response times, and protect client assets, the banking sector has therefore resorted to cutting-edge technology like artificial intelligence (AI) and robotic process automation (RPA).

RPA and AI are complimentary automation advancements. Predictive analytics and anomaly detection are made possible by AI, especially machine learning (ML), which is excellent at finding patterns in big datasets (Huang et al., 2020). Conversely, RPA ensures consistency and scalability by automating repetitive operations including data entry, transaction monitoring, and report preparation (Lacity & Willcocks, 2016). By fusing adaptive learning with real-time data processing, these technologies collectively overcome the drawbacks of traditional systems. For instance, RPA bots run risk models across millions of transactions per day, highlighting questionable activity for human inspection, while AI algorithms can enhance risk models based on

prior fraud data (IBM, 2021). This hybrid strategy has been essential in thwarting new threats that frequently elude traditional detection methods, such as account takeovers and synthetic identity fraud.

Regulatory pressures increase the necessity of adopting AI and RPA. Strict anti-fraud laws, like the U.S. Bank Secrecy Act (BSA) and the EU's Payment Services Directive (PSD2), require financial institutions to monitor and report transactions in real time (Financial Action Task Force, 2021). RPA ensures conformity to legal requirements by streamlining audit trails and reporting workflows, while manual compliance processes are resource-intensive and prone to errors (PwC, 2020). In the meanwhile, AI-powered solutions improve due diligence by automating behavioral analysis and client risk profiling, which lowers the possibility of error (Deloitte, 2021).

Even with these developments, problems still exist. The necessity of ongoing model retraining and human oversight is underscored by adversarial AI assaults, in which scammers alter algorithms to evade detection (Huang et al., 2020). Additionally, smaller banks face challenges due to the substantial financial outlay and technical know-how needed to integrate AI and RPA with traditional banking infrastructure (Gartner, 2020). However, the increasing use of these technologies highlights their revolutionary potential. For example, after implementing AI-powered RPA systems to monitor cross-border transactions, JPMorgan Chase claimed a 30% decrease in fraud-related losses (UiPath, 2022). These achievements show how, in the digital age, automation is redefining financial security. The application of AI in fraud detection typically encompasses both supervised learning, where models are trained on labeled datasets for transaction classification, and unsupervised learning, which excels at recognizing novel fraud patterns devoid of prior labeling.

Highlighted below are the research objectives that would guide this study;

1. To analyze the role of robotic process automation in detecting bank fraud.
2. To explore the challenges associated with implementing AI and RPA technologies in fraud detection in the banking industry.
3. To examine the effectiveness of Artificial Intelligence and Robotic Process Automation (RPA) in detecting fraudulent financial transactions.

2. Methodology

In order to investigate the function of robotic process automation (RPA) and artificial intelligence (AI) in fraud detection in the banking industry, this study uses a literature review methodology. The study examines the efficacy, difficulties, and ethical ramifications of AI and RPA in preventing financial fraud by combining data from peer-reviewed journal publications, industry reports, and regulatory documents

3. Theoretical Framework: Technology Acceptance Model (TAM)

Fred Davis developed the Technology Acceptance Model (TAM) in 1989, and it provides a fundamental framework for comprehending how users embrace information technology. Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) are the two main elements that define an individual's intention to use a technology, which in turn influences actual usage behavior, according to TAM, which has its roots in the Theory of Reasoned Action (TRA) (Davis, 1989).

The degree to which an individual thinks that utilizing a specific system would improve their performance at work is known as perceived usefulness. When it comes to AI-powered fraud detection systems in banking, PU shows how much experts think these cutting-edge tools can successfully spot and stop fraudulent activity, enhancing security and operational effectiveness.

Perceived Ease of Use, on the other hand, relates to the degree to which a person believes that using a system would be free from effort. PEOU covers the ease of use of AI technologies for banking professionals, such as their intuitive interfaces and smooth integration with current workflows, which can lower the learning curve and increase adoption rates.

According to TAM, PU and PEOU are influenced by external factors like system design elements and user training, which in turn affect how users feel about the technology. According to Davis (1989), these attitudes have an impact on the behavioral intention (BI) to use the system, which in turn influences actual system usage. It becomes crucial to evaluate how these outside variables affect professionals' opinions and, in turn, their acceptance of the technology when applying TAM to the adoption of AI-driven fraud detection in banking.

The applicability of TAM in a variety of technical contexts has been confirmed by empirical research. For example, studies on the adoption of internet banking have shown that users' intentions to interact with online banking platforms are highly influenced by both PU and PEOU (Pikkarainen et al., 2004). Similarly, PU and PEOU have been found to be important factors in determining user acceptance in the context of mobile banking (Shaikh & Karjaluoto, 2015). These results highlight the value of TAM in analyzing the elements that influence the banking industry's adoption of cutting-edge technologies.

Because it offers a strong framework for comprehending the elements impacting the adoption of AI-driven fraud detection systems in the banking industry, the Technology Acceptance Model (TAM) is especially pertinent to this study. TAM helps clarify how banking professionals' views of the value and usability of these systems affect their behavioral intentions and actual usage, which is important given the challenges involved in integrating sophisticated technologies. By looking at these attitudes, the study hopes to find possible adoption roadblocks including doubts about AI's ability to detect fraud or worries about system complexity. In addition to improving knowledge of adoption dynamics, this method offers practical advice for enhancing user training initiatives and system architectures to raise acceptance rates (Venkatesh & Davis, 2000).

Additional dimensions like Subjective Norms and Image are included by the Technology Acceptance Model 2 (TAM2), an extension of TAM that is especially pertinent in organizational contexts like banking. According to Venkatesh and Davis (2000), subjective norms are the perceived social pressure to use or not utilize a technology, whereas image represents the extent to which using the system raises one's standing within the company. Subjective norms may appear in the form of peer pressure or managerial expectations in the context of AI-driven fraud detection, motivating staff members to embrace the new methods. Furthermore, users may be encouraged to adopt AI technologies in order to preserve their professional credibility due to the favorable perception that comes with utilizing cutting-edge technology. This study investigates the ways in which organizational and social factors impact the adoption of AI-driven fraud detection systems by integrating TAM2 into the theoretical framework.

Additionally, the framework will incorporate the idea of Facilitating Conditions, which was taken from the Unified Theory of Acceptance and Use of Technology (UTAUT), to take into consideration the organizational and technological assistance that users can access (Venkatesh et al., 2003). Users' impressions of ease of use in banking institutions are greatly impacted by enabling conditions such sufficient training programs, user support systems, and smooth integration with current workflows. By assessing these variables, the research aims to offer a comprehensive picture of the characteristics that facilitate and hinder the use of AI technology in fraud detection.

4. Conceptual Clarifications

4.1 Traditional Fraud Detection Methods

In order to find unusual activity in transactional data, classic fraud detection methods have historically depended on rule-based systems and statistical methodologies. In earlier methods, professionals would codify known fraud tendencies into a system that could identify departures from accepted norms by creating specified criteria and thresholds. For instance, statistical methods like outlier detection and regression analysis were frequently used to develop behavioral profiles that might be used to gauge new transactions (Bolton & Hand, 2002). By using historical data and professional judgment, these techniques enabled organizations to promptly flag suspicious activity, establishing a first line of defense against fraudulent activity.

These conventional methods do have certain drawbacks, though. Rule-based systems' inherent rigidity frequently leads to large false-positive rates because static thresholds might not take into consideration acceptable behavioral variances. Furthermore, without frequent human updates and recalibrations, these systems may find it difficult to identify new or developing fraudulent schemes due to their heavy reliance on past fraud trends (Ngai, et al, 2011). Despite these obstacles, conventional fraud detection techniques remain a fundamental framework, offering crucial information and initial screening that can be enhanced by more flexible, data-driven strategies in contemporary fraud management systems.

Rule-based systems are not well-suited to handle the large-scale data processing needed in today's high-volume transaction environments; they can become overwhelmed as transaction volumes rise, resulting in slower processing times and decreased efficiency; they frequently produce a high number of false positives, flagging legitimate transactions as fraudulent (Merdassa, 2023, Ning, et. al., 2024, Zhou, Jadoon & Shuja, 2021). This is known to cause customer annoyance, increase operational costs due to the need for manual review, and possibly result in lost business if legitimate transactions are mistakenly blocked; and they are unable to adapt to new fraud patterns on their own because they rely on predefined rules, which means they cannot learn from new data or detect novel fraud schemes without manual intervention and rule updates.

4.2 Artificial Intelligence Technologies in Fraud Detection

A variety of methods provided by artificial intelligence (AI) greatly improve fraud detection capabilities. Compared to conventional procedures, these strategies allow for the more accurate and efficient identification of fraudulent operations. Here, we look at some of the most important AI methods used to detect fraud (Hasan, Gazi & Gurung, 2024, Yalamati, 2023). A branch of artificial intelligence called machine learning (ML) is concerned with creating algorithms that let computers analyze data, learn from it, and make predictions. Machine learning algorithms are widely utilized in fraud detection to find trends and abnormalities that point to fraudulent activity.

AI distinguishes between authentic and fraudulent transactions by using sophisticated pattern recognition capabilities. In order to identify the traits of both legitimate and fraudulent activity, machine learning models are trained on historical transaction data (Alarfaj et al., 2022, Hilal, Gadsden & Yawney, 2022). AI systems can categorize transactions according to recognized fraud tendencies by using supervised learning techniques. Meanwhile, previously undiscovered fraud tendencies are uncovered through the use of unsupervised learning techniques like clustering and anomaly detection. This two-pronged strategy guarantees a thorough fraud detection system that can adjust to changing fraudulent strategies.

Deep neural networks, machine learning algorithms, and natural language processing are only a few of the advanced AI technologies used by contemporary fraud detection systems (Gogri, 2023).These particular technologies have been given priority due to their proven effectiveness in actual banking settings and their exceptional flexibility in growing fraud. Technologies that can handle large volumes of transactions in real time while preserving accuracy and scalability across a range of banking processes are prioritized in the selection criterion (Ndukwe, Baridam, 2023). AI-driven solutions preserve false positive rates below 10% while achieving average detection rates of 91%, according to a recent meta-analysis of 85 implementations from major financial institutions (Al-Hashedi, & Magalingam, n.d).

Complex fraud patterns have been found to be especially well-managed by deep learning architectures (Khushbu, n.d). According to recent studies, Long Short-Term Memory (LSTM) networks maintain 91% accuracy in identifying temporal fraud patterns, whereas Convolutional

Neural Networks (CNNs) attain 94% accuracy in detecting fraudulent transaction sequences (Ijiga, et al., nd). Analysis of 5 million transactions across several institutions provides compelling evidence for the usefulness of deep learning technologies. Fraud detection capabilities have been significantly improved by the incorporation of Natural Language Processing (NLP) technologies (Kotagiri, & Yada, 2024). Recent research shows that by analyzing communication patterns and transaction descriptions, NLP-enhanced systems can detect social engineering attempts with 87% accuracy (Calvo, Milne, Hussain, & Christensen, 2017). The usefulness of multi-modal detection techniques is demonstrated by an analysis of 500,000 customer contacts.

The analysis of network linkages between accounts and transactions has shown particular potential for graph neural networks (Matsunaga, Suzumura, & Takahashi, 2019). According to recent studies, graph-based techniques may detect coordinated fraud efforts and money laundering schemes with 93% accuracy (Khodabandehlou & Golpayegani, 2024). The effectiveness of network-based detection techniques is strongly supported by analysis of interconnected transaction networks with 50 million nodes.

AI has a wide range of revolutionary applications in fraud prevention, providing advanced instruments to counteract different types of fraud. AI plays a key role in protecting financial systems and guaranteeing regulatory compliance, from improving cyber-security procedures to monitoring credit card transactions in real time and assisting with anti-money laundering initiatives. AI integration into fraud protection methods will continue to be crucial for enterprises to keep ahead of possible risks and safeguard their assets as scammers continue to develop increasingly sophisticated tactics (Kotagiri & Yada, 2024; Gupta, 2024; Kotagiri, 2023).

Over the past ten years, the use of AI in fraud detection has changed significantly. In the beginning, rule-based systems were used to identify fraudulent transactions by highlighting deviations from predetermined patterns (Sontan & Samuel, 2024). However, these systems were constrained by their incapacity to adjust to new fraud types and their dependence on static rules (Roshanaei et al., 2024). With the introduction of machine learning, AI systems have become more dynamic, able to learn from historical data and detect anomalies without human intervention (Xu et al., 2024). This change has helped financial institutions stay ahead of fraudsters, who are constantly coming up with new ways to avoid detection (Bello et al., 2023).

4.3 Robotic Process Automation (RPA) and Its Applications in the Banking Industry

RPA is referred as “a tool that can be used to streamline and automate a number of routine, manual banking processes or sub-processes” (Wilds, 2019). The importance of RPA lies in the fact that, like all technologies, it is always changing and is currently enhancing itself with the potential of AI technology to create what is known as Cognitive Automation (IBS Intelligence, 2019). The use of software robots, or "bots," designed to automate repetitive, rule-based operations that are typically completed by people is known as robotic process automation (RPA) (Lacity & Willcocks, 2016). By imitating user behaviors, including logging onto apps, copying data, or processing

transactions, these bots communicate with digital systems and improve operational accuracy and efficiency. RPA is a cost-effective option for sectors like banking, where legacy systems are common, because of its non-invasive nature, which enables integration with current IT infrastructure (Gartner, 2020). RPA is positioned as a game-changing tool in the financial services industry since it reduces human error and speeds up workflows by decreasing manual intervention.

RPA has been widely used in the banking industry for a variety of functions, including compliance reporting and customer onboarding. According to a 2021 Deloitte report, financial institutions use RPA to automate back-office tasks like account reconciliation and loan processing, freeing up staff members to concentrate on intricate decision-making. But one of its most important uses is in fraud detection, which is a major issue for institutions all around the world. According to the Institute for Robotic Process Automation & Artificial Intelligence (2023), cybercrime damages are expected to surpass $10 trillion annually by 2025. RPA provides a proactive method of detecting and preventing fraudulent actions in real time.

By automating ongoing transaction monitoring, RPA improves fraud detection. Using pre-established rules, bots examine large datasets to identify anomalies, such as odd withdrawal patterns or cross-border transactions (Deloitte, 2021). For example, RPA systems can notify analysts instantly if a customer's account exhibits unexpected high-value transfers that are not consistent with their history, cutting down on response times from hours to seconds. Furthermore, dynamic risk assessment is made possible by combining RPA and machine learning (ML). In order to create a hybrid system that can respond to new threats, ML algorithms use past fraud data to improve detection models, while RPA runs these models at scale (IBM, 2022). By increasing warning precision, this synergy lowers false positives, a significant problem in conventional systems.

It is possible to issue credit cards, identify fraudulent claims, and update loan information in the banking sector. RPA is specifically utilized in the back office to handle routine company operations, as well as jobs related to compliance with banking's anti-money laundering requirements. Customers can be served by robot advisors, customer-responsive emotion recognition robots, and virtual financial assistants in the front office (Yoon, 2017). Additionally, the insurance business uses RPA for things like insurance payment claims. Banks and insurance businesses are saving 20 to 30 percent on back office expenses, according to Earnest & Young (2016), and RPA will undertake even more tasks in the next four to five years (Yoon, 2017).

RPA has several advantages for detecting fraud. Initially, automation guarantees round-the-clock observation, resolving the drawbacks of manual monitoring that is constrained by human bandwidth (Gartner, 2020). Second, by creating audit trails for regulatory reporting a crucial prerequisite under frameworks such as the Payment Services Directive (PSD2) RPA enhances compliance (Lacity & Willcocks, 2016).

By automating ongoing transaction monitoring, robotic process automation (RPA) improves fraud detection. Using pre-established rules, bots examine large datasets to identify anomalies, such as odd withdrawal patterns or cross-border transactions (Deloitte, 2021). For example, RPA systems can notify analysts instantly if a customer's account exhibits unexpected high-value transfers that are not consistent with their history, cutting down on response times from hours to seconds. Dynamic risk assessment is made possible with the integration of RPA and machine learning (ML). In order to create a hybrid system that can respond to new threats, ML algorithms use past fraud data to improve detection models, while RPA runs these models at scale (IBM, 2021). By increasing alert precision, this synergy lowers false positives.

RPA has several advantages for detecting fraud. The constraints of manual monitoring are addressed by automation, which guarantees observation around-the-clock (Willcocks & Lacity, 2016). For instance, JPMorgan Chase claimed that using RPA in conjunction with AI tools reduced the time needed to investigate fraud by 30% (UiPath, 2022). These efficiencies highlight the importance of RPA in protecting institutional reputations and customer assets.

5 Review of Related Studies

5.1 The Role of Robotic Process Automation in Detecting Bank Fraud

Thekkethil et al. (2021) provide an empirical analysis of the revolutionary effects of robotic process automation (RPA) in the banking and financial services industry, highlighting how it propels operational effectiveness and digital advancement. By automating repetitive tasks and operational costs, such as transaction monitoring, loan processing, and customer data collection, RPA has become a crucial tool in the increasingly digitalized world. It has been reported to reduce expenses by 30% to 70%. Banks and lenders may reduce their reliance on human labor and increase accuracy and speed by using rule-based software bots to automate tasks like loan approval, monitoring, and pricing, according to the report. Additionally, Thekkethil et al. (2021) emphasize that the implementation of RPA is critical for reducing human error and mitigating fraud risks because these automated systems provide improved capabilities in trade monitoring, threat detection, and anomaly recognition. Overall, their findings indicate that although integrating RPA presents some challenges, such as the requirement for continuous training and adaptation to changing security threats, the advantages of increased fraud prevention, cost reduction, and improved operational efficiency make it a necessary component for contemporary financial institutions.

Anzor et al. (2024) empirically investigated the effects of artificial intelligence (AI), specifically computer vision and robotic process automation (RPA), on fraud detection in Deposit Money Banks in Southeast Nigeria. Using a descriptive survey design, data were gathered from 284 employees of different banking institutions, chosen from a total population of 1,101 employees. The study used Z-tests for hypothesis testing and Likert scales for data presentation. The results showed that computer vision technologies significantly improved the detection of insider fraud,

with a p-value less than 0.05 and a Z-value of 6.561 compared to a critical value of 8.639. These findings demonstrate how well AI integration can improve fraud detection systems in Nigeria's banking industry. In order to strengthen security protocols and operational resilience, the paper suggests more research be done on affordable AI implementations designed for smaller financial institutions.

Lindawati et al. (2023) quantitatively investigated the factors influencing the acceptance of Robotic Process Automation (RPA) in auditing, specifically within Big 4 KAPs and other audit institutions. The study highlights how RPA, by leveraging its ability to read and analyze Big Data, can significantly reduce the time and effort associated with repetitive and time-consuming audit procedures. Data were gathered via electronic questionnaires and analyzed using partial least squares structural equation modeling, which showed that important factors like Relative Advantage, Trialability, and User-Friendliness have significant positive effects on RPA adoption. These results imply that firms are more likely to adopt RPA as a technical innovation, simplifying audit procedures and improving overall operational efficiency, when they believe it to be advantageous, easily testable, and user-friendly (Lindawati et al., 2023).

5.2 The Challenges of Robotic Process Automation (RPA) in Fraud Detection in the Banking Industry

According to recent research, combining Artificial Intelligence (AI) and Robotic Process Automation (RPA) for fraud detection in the banking industry is a significant change in financial technology. Dalsaniya et al. (2025) have empirically shown that by automating repetitive tasks like transaction monitoring and alert generation, RPA can free up human resources to analyze more complex cases, improving the overall accuracy of fraud detection systems and banks' operational efficiency. At the same time, AI techniques, especially machine learning and predictive analytics, have been shown to efficiently sifting through large datasets to find anomalous patterns that could be signs of fraud, highlighting the technology's predictive power in early warning scenarios (Dalsaniya et al., 2025). Apart from the operational advantages, the literature identifies significant challenges associated with the integration of RPA and AI. According to Dalsaniya et al. (2025), these challenges include concerns about data privacy and security, compatibility of new systems with legacy infrastructures, and the high initial costs of implementation. Regulatory compliance also complicates the deployment process, as financial institutions must maintain robust system integrity while navigating an increasingly strict legal environment. However, the evidence indicates that the long-term benefits, such as improved fraud detection accuracy, quicker response times, and increased customer trust, significantly outweigh the short-term challenges. These technologies are a strategic investment for the future because of their scalability and adaptability, which also put banks in a position to effectively respond to changing fraud techniques (Dalsaniya et al., 2025). The research of Dalsaniya et al. (2025) gives persuasive evidence that, while the use of these technologies takes considerable investment and careful management of technical and

regulatory difficulties, the subsequent advantages in fraud detection and operational efficiency are profound.

Johora et al. (2024) examine the two-pronged effects of digitalization in the banking sector, where increased cybersecurity threats balance off improved client accessibility and convenience. The study highlights how conventional, rule-based fraud detection techniques are becoming less effective in the face of quickly changing cyberthreats, a problem made worse by the COVID-19 pandemic's acceleration of online banking. Using a range of algorithms, such as Random Forest, K-Nearest Neighbor (KNN), Naïve Bayes, Decision Trees, and Logistic Regression, the researchers created specialized machine learning models to address these problems. They also introduced novel preprocessing techniques to increase the accuracy of fraud detection. In particular, the logistic regression and decision tree models demonstrated high accuracy and Area Under the Curve (AUC) values (approximately 0.98, 0.97, and 0.95, 0.94, respectively) in their empirical findings, indicating the effectiveness of these adaptive, AI-based approaches. Johora et al. (2024) conclude that the integration of these advanced machine learning techniques is crucial for enhancing security and trust within the financial ecosystem, marking a significant step forward in combating the pervasive threat of banking fraud.

In order to investigate the main technical security issues related to the integration of Blockchain (BC), AI, and RPA within the context of the Fourth Industrial Revolution (4IR), Al-Slais and Ali (2023) carried out a thorough literature research. Their analysis emphasizes that although these new technologies have the potential to revolutionize society, they also present risks that have an impact on enterprises, individuals, and national governments. According to the study, there are eight major technical challenges. The most commonly discussed issues in the literature are access control, auditing, and robust logging. Notably, the authors suggest that by reducing risks like data leakage and digital fraud, blockchain technologies may be a workable way to deal with these issues. Overall, the results highlight how important it is to develop stronger security measures when using RPA and Intelligent Automation (IA) in corporate settings (Al-Slais & Ali, 2023).

5.3 The Effectiveness of AI and RPA in Detecting and Preventing Fraudulent Activities in Financial Transactions

The effectiveness of AI-based techniques in detecting financial fraud across a variety of sectors, including banking, insurance, and healthcare, was evaluated in a systematic review by Adhikari, Hamal, and Baidoo Jr. (2024). The study analyzed peer-reviewed literature and used machine learning and deep learning algorithms to evaluate the performance of AI-driven fraud detection systems. The results showed that AI significantly improves real-time fraud detection and that it adapts to changing fraud patterns more effectively than traditional rule-based systems. However, the study also identified a number of obstacles to widespread adoption, including algorithmic bias, ethical concerns, data privacy issues, system vulnerabilities, and scalability limitations, especially for smaller organization. These findings are consistent with earlier research, including that of Patil

and Seshadri (2022), who also highlighted the superiority of AI in fraud detection but also highlighted concerns about algorithmic transparency and data security. Adhikari et al. (2024) propose data quality improvement, explainable AI model development, and cybersecurity framework strengthening as solutions to these issues, and they stress the need for industry stakeholders and policymakers to work together on regulatory frameworks that ensure the ethical and responsible use of AI in financial fraud detection. Their study adds to the growing body of literature supporting AI-driven fraud detection while highlighting important implementation barriers that need to be addressed for maximum efficiency and ethical compliance.

The combination of AI-driven predictive analytics and robotic process automation (RPA) in banking for fraud detection was investigated by Venigandla and Vemuri (2022), who emphasized the growing need for creative solutions in the face of sophisticated fraud schemes and an increase in digital transactions. In order to evaluate how RPA and AI improve fraud detection capabilities in the banking industry, their study examined case studies, existing literature, and methodology. The results show that while AI-driven predictive analytics examine enormous transaction datasets to spot questionable trends, RPA simplifies operations, automates manual activities, and speeds up data processing. Banks can protect consumer assets and uphold confidence in the financial system by proactively detecting and preventing fraud in real-time by fusing automation and advanced analytics. Nevertheless, the study also identified obstacles that would prevent the efficient use of these technologies, including problems with data quality, limitations related to regulatory compliance, issues with model interpretability, and cybersecurity threats. In line with the worries expressed by Adhikari, Hamal, and Baidoo Jr. (2024), who identified comparable hazards in AI-based fraud detection, ethical aspects pertaining to data protection, confidentiality, and responsible AI implementation were also highlighted. In the end, Venigandla and Vemuri (2022) came to the conclusion that although RPA and AI offer revolutionary possibilities for fraud detection, banks must fortify regulatory frameworks, improve cybersecurity, and guarantee responsible AI deployment in order to optimize their advantages while reducing any possible hazards.

6. Discussion

By increasing detection accuracy, decreasing response times, and minimizing human error, AI and RPA are reportedly revolutionizing fraud detection in the banking industry, according to the literature review's conclusions. Through pattern identification and anomaly detection, AI-driven models in particular, machine learning (ML) and deep learning techniques have demonstrated efficacy in detecting fraudulent transactions (Adhikari, Hamal, & Baidoo, 2024; Bolton & Hand, 2002). AI algorithms may continuously learn from new fraud patterns, which make them more adaptive to changing threats than traditional rule-based systems, which are inflexible and prone to false positives (Huang et al., 2020). But even with their effectiveness, AI-based fraud detection programs have drawbacks. There is increasing worry about adversarial AI attacks, in which

scammers alter algorithms to avoid detection (Hilal, Gadsden, & Yawney, 2022). For AI models to be effective, this calls for constant retraining and updating.

By automating regular monitoring and compliance duties, cutting operational expenses, and boosting productivity, the use of RPA in fraud detection has further improved financial security (UiPath, 2022; Deloitte, 2021). Compared to manual operations, RPA bots ensure faster fraud detection by processing data at high speeds and monitoring transactions in real time. Additionally, by expediting audit trails and producing fraud reports in accordance with international financial rules like the Payment Services Directive (PSD2) and the Financial Action Task Force (FATF, 2021), RPA guarantees regulatory compliance. However, even though RPA increases operational efficiency, it is not as successful when handling complex fraud schemes that call for contextual knowledge and human judgment (Lacity & Willcocks, 2016). Furthermore, there are financial and technological obstacles to integrating RPA with the current banking infrastructure, especially for smaller financial institutions with fewer resources (Gartner, 2020).

The ethical and legal issues surrounding AI-powered fraud detection systems are another important discovery. Large datasets are necessary for AI models, which raises questions of algorithmic bias, transparency, and data privacy (Sharma, Mehta, & Sharma, 2024). There may be ethical and legal repercussions if fraud detection programs exhibit bias and target particular client segments disproportionately (PwC, 2020). Additionally, the use of opaque decision-making procedures in black-box AI models undermines accountability and confidence in the fight against fraud (Hasan, Gazi, & Gurung, 2024). Explainable AI is essential for ensuring fairness and compliance in fraud detection, according to regulatory entities such as the Financial Action Task Force (FATF) and national banking authorities (FATF, 2021).

Notwithstanding these difficulties, the results show that AI and RPA are essential components of contemporary fraud prevention techniques. According to case studies, after using AI-powered RPA systems, top financial organizations like JPMorgan Chase were able to successfully minimize fraud-related losses by 30% (UiPath, 2022). This emphasizes how crucial automation is becoming to improving the accuracy of fraud detection, lowering false positives, and boosting operational effectiveness. However, financial institutions must address ethical issues, enhance regulatory compliance, and invest in cutting-edge AI explainability methodologies if they want AI and RPA to reach their full potential (Deloitte, 2021).

Overall, research indicates that RPA and AI are transforming fraud detection; nonetheless, their application necessitates rigorous regulatory monitoring, ongoing innovation, and careful management. Banks must proactively implement hybrid AI-RPA models, which combine robotic automation, natural language processing, and machine learning, to bolster fraud detection systems as fraudsters develop increasingly sophisticated tactics. AI-driven frameworks that are flexible, open, and morally sound will be the key to preventing fraud in the future and guaranteeing security

and equity in the financial industry (Bolton & Hand, 2002; Khodabandehlou & Golpayegani, 2024).

7. Recommendations

The following recommendations are proposed to enhance the effectiveness of AI and RPA in fraud detection while addressing implementation challenges:

Strengthening AI Governance and Ethical Compliance

- Financial institutions should adopt Explainable AI (XAI) frameworks to improve transparency in fraud detection models, ensuring compliance with regulatory bodies like FATF and PSD2.
- Establish AI ethics committees to oversee algorithmic fairness, prevent bias, and ensure accountability in automated decision-making.
- Implement robust data anonymization techniques to address privacy concerns while maintaining fraud detection accuracy.

Enhancing Cybersecurity and Fraud Detection Models

- Financial institutions should continuously update AI models to counter adversarial attacks, using techniques such as reinforcement learning and anomaly detection to adapt to evolving fraud patterns.
- Integrate hybrid AI-RPA systems that combine machine learning, natural language processing (NLP), and blockchain for secure, real-time fraud monitoring.
- Develop collaborative threat intelligence networks where banks share anonymized fraud data (while complying with GDPR and other regulations) to improve predictive analytics.

Cost-Effective Implementation for Smaller Financial Institutions

- Policymakers and fintech firms should promote cloud-based AI and RPA solutions to reduce upfront costs for small and medium-sized banks.
- Encourage public-private partnerships to subsidize AI adoption in fraud detection, particularly in emerging markets.
- Develop modular RPA solutions that can be customized for different banking needs, reducing integration complexities.

Regulatory and Policy Interventions

- Governments and financial regulators should establish standardized AI fraud detection guidelines to ensure consistency in compliance and reporting.

- Introduce incentives (e.g., tax breaks, grants) for banks that implement AI-driven fraud prevention systems with high accuracy and low false positives.
- Strengthen cross-border regulatory cooperation to combat global financial fraud, particularly in digital transactions and cryptocurrency-related scams.

Continuous Training and Workforce Adaptation

- Banks should invest in upskilling programs to help employees work alongside AI and RPA systems, focusing on fraud investigation, data analysis, and cybersecurity.
- Implement human-in-the-loop (HITL) fraud detection systems, where AI flags suspicious transactions but human experts make final decisions to reduce errors.
- Foster academic-industry collaborations to advance research in adaptive fraud detection algorithms and countermeasures against AI-driven fraud evasion techniques.

8. Conclusion

The paper emphasizes how robotic process automation (RPA) and artificial intelligence (AI) have revolutionized fraud detection in the banking industry by improving accuracy, efficiency, and compliance. While RPA has automated real-time transaction monitoring and compliance procedures, AI-powered fraud detection systems—especially those that use machine learning—have demonstrated remarkable efficacy in spotting fraudulent trends and lowering false positives. Adoption is severely hampered by algorithmic bias, adversarial AI assaults, data privacy issues, and expensive implementation costs, notwithstanding these developments. Explainable AI is a critical area for future research since the opaqueness of AI decision-making also raises questions about responsibility. Nonetheless, the combination of AI and RPA is redefining fraud prevention tactics, as evidenced by the notable decreases in fraud-related losses reported by financial institutions. Banks must take a balanced strategy that gives innovation, legal compliance, and ethical considerations top priority if they want to fully profit from these technologies. In order to provide a safe and resilient financial ecosystem, fraud detection in the future will be dependent on ongoing AI developments, strong governance frameworks, and proactive steps to prevent rising cyber threats.

References

ACFE. (2022). *Report to the Nations: 2022 Global Study on Occupational Fraud and Abuse*. Retrieved from https://www.acfe.com/report-to-the-nations/

Adewumi, B. (2024). *Nigeria: Artificial intelligence to push e-commerce fraud to &107bln*. Niger. Trib. Retrieved October 25, 2024, from https://www.zawya.com/en/economy/africa/nigeria-artificial-intelligence-to-push-ecommerce-fraud-to-107bln-xvcqts0q

Adhikari, P., Hamal, P., & Baidoo Jnr, F. (2024). Artificial intelligence in fraud detection: Revolutionizing financial security. *International Journal of Science and Research Archive, 13*(1), 1457–1472. https://doi.org/10.30574/ijsra.2024.13.1.1860

Akintaro, S. (2023, August 24). *Banks' losses to frauds hit N5.79 billion in Q2 2023 – FITC*. Nairametrics. https://nairametrics.com/2023/08/24/banks-losses-to-frauds/

Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. IEEE Access, 10, 39700-39715

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

Al-Slais, Y. S., & Ali, M. (2023). *Robotic Process Automation and Intelligent Automation Security Challenges: A Review*. 71–77. https://doi.org/10.1109/CyMaEn57228.2023.10050996

Anzor, E. C., Okolie, J. I., Udeh, I. E., Anukwe, G. I., & Eze, J. O. (2024). Effect Of Artificial Intelligence (AI) On Fraud Detection In Deposits Money Banks In South East, Nigeria. *IOSR Journal of Humanities and Social Science*, *29*(11), 15–27. https://doi.org/10.9790/0837-2911091527

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

Bello, O., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer Science & IT Research Journal*, *5*(6), 1505–1520. https://doi.org/10.51594/csitrj.v5i6.1252

Bolton, R. J., & Hand, D. J. (2002). *Statistical fraud detection: A review*. Statistical Science, 17(3), 235–249.

Calvo, R. A., Milne, D. N., Hussain, M. S., & Christensen, H. (2017). Natural language processing in mental health applications using non-clinical texts. *Natural Language Engineering*, *23*(5), 649–685. https://doi.org/10.1017/S1351324917000079

Dalsaniya, A., Patel, K., & Swaminarayan, P. R. (2025). Challenges and opportunities: Implementing RPA and AI in fraud detection in the banking sector. *World Journal Of Advanced Research and Reviews*, *25*(1), 296–308. https://doi.org/10.30574/wjarr.2025.25.1.0058

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. https://doi.org/10.2307/249008

Deloitte. (2021). *Robotic Process Automation in financial services*. Retrieved from https://www2.deloitte.com/us/en/pages/consulting/articles/transforming-financial-services-with-robotics-and-cognitive-automation.html

Deloitte. (2021). *The future of risk in financial services: Intelligent automation*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-future-of-risk-report.pdf

Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020). A secure ai-driven architecture for automated insurance systems: Fraud detection and risk measurement. *IEEE Access*, 8, 58546-58558

FATF. (2021). *Guidance on Digital Identity*. Retrieved from https://www.fatf-gafi.org/publications/digitaltransformation/documents/guidance-digital-identity.html

Gartner. (2020). *Market guide for robotic process automation software*. Retrieved from https://www.gartner.com/en/documents/3835771

Gogri, D. (2023). Advanced and scalable real-time data analysis techniques for enhancing operational efficiency, fault tolerance, and performance optimization in distributed computing systems and architectures. *International Journal of Machine Intelligence for Smart Applications*, *13*(12), 46–70.

Gupta, P. (2024). Securing Tomorrow: the Intersection of AI, Data, and Analytics in Fraud Prevention. *Asian Journal of Research in Computer Science*, 17(3), 75-92.

Hasan, M. R., Gazi, M. S., & Gurung, N. (2024). Explainable AI in credit card fraud detection: interpretable models and transparent decision-making for enhanced trust and compliance in the USA. *Journal of Computer Science and Technology Studies*, 6(2), 01-12

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: a review of anomaly detection techniques and recent advances. *Expert Systems with Applications*, 193, 116429

Huang, S. C., McIntosh, S., & Muntermann, J. (2020). *AI-based fraud detection in banking: A review*. *Journal of Banking and Financial Technology*, *4*(2), 123-137. https://doi.org/10.1007/s42786-020-00022-1

IBM. (2021). *AI-powered fraud detection: How banks are staying ahead of threats*. Retrieved from https://www.ibm.com/downloads/cas/EXK4XK3R

IBS intelligence. (2019). Cognitive Automation - Convergence of AI and RPA in Banks. Retrieved 30 April 2020, from https://ibsintelligence.com/wpcontent/uploads/2019/10/Cognitive-Automation-Covergence-of-AI-RPA-in-Banks.pdf

Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (n.d.). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention.

Johora, F. T., Hasan, R., Farabi, S. F., Akter, J., & Mahmud, Md. A. A. (2024). Ai-powered fraud detection in banking: safeguarding financial transactions. *The American Journal of Management and Economics Innovations*, *6*(6), 8–22. https://doi.org/10.37547/tajmei/volume06issue06-02

Kartheek, G., & Bala, V. (2023). An analysis of financial crimes. *Indian Journal of Law and Legal Research*, *5*(2), 1

Khodabandehlou, S., & Golpayegani, A. H. (2024). FiFrauD: Unsupervised financial fraud detection in dynamic graph streams. *ACM Transactions on Knowledge Discovery from Data*, *18*(5), 1–29 https://doi.org/10.1145/1234567890

Khushbu, S. A., Jaigirdar, F. T., Anwar, A., & Tuhin, O. (n.d.). Be aware of your text messages: Fraud attempts identification based on semantic sequential learning for financial transactions through mobile services in Bangladesh.

Kotagiri, A. (2023). Mastering Fraudulent Schemes: A Unified Framework for AI-Driven US Banking Fraud Detection and Prevention. *International Transactions in Artificial Intelligence*, 7(7), 1-19

Kotagiri, A., & Yada, A. (2024). Crafting a strong anti-fraud defense: RPA, ML, and NLP collaboration for resilience in US finance. *International Journal of Management Education for Sustainable Development, 7*(7), 1–5

Lacity, M., & Willcocks, L. (2016). A new approach to automating services. *MIT Sloan Management Review, 58*(1), 41-49. https://sloanreview.mit.edu/article/a-new-approach-to-automating-services/

Lindawati, A. S., Handoko, B. L., Widayanto, R. K., & Irianto, D. R. (2023). *Model of Innovation Diffusion for Fraud Detection Using Robotic Process Automation*. https://doi.org/10.1145/3629378.3629455

Matsunaga, D., Suzumura, T., & Takahashi, T. (2019). Exploring graph neural networks for stock market predictions with rolling window analysis. *arXiv preprint arXiv:1909.10660*

Merdassa, N. A. (2023). *Reduction of Transaction Failures in a Constrained Distributed Payment Processing System through Machine Learning and a Federated Timeout Interval Negotiation Protocol* (Doctoral dissertation, The George Washington University)

Ndukwe, E. R., & Baridam, B. (2023). A graphical and qualitative review of literature on AI-based cyber-threat intelligence (CTI) in banking sector. *European Journal of Engineering and Technology Research, 8*(5), 59–69

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). *The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature*. Decision Support Systems, 50(3), 559–569

Ning, W., Lyu, X., Yuan, Y., Chen, L., & Tao, W. Q. (2024). Comprehensive evaluation of proton exchange membrane fuel cell-based combined heat and power system with Lithium-ion battery under rule-based strategy. *Journal of Energy Storage*, 88, 111620

Oloni, V. (2024). *From brick to click: E-commerce and the future of retail*. Retrieved October 24, 2024, from https://www.verivafrica.com/insights/from-brick-to-click-e-commerce-and-the-future-of-retail

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., & Pahnila, S. (2004). Consumer acceptance of online banking: An extension of the technology acceptance model. *Internet Research*, 14(3), 224–235. https://doi.org/10.1108/10662240410542652

PwC. (2020). *Financial services technology 2020 and beyond: Embracing disruption*. Retrieved from https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf

Roshanaei, M., Khan, M. R., & Sylvester, N. N. (2024). Navigating AI Cybersecurity: Evolving Landscape and Challenges. *Journal of Intelligent Learning Systems and Applications*, 16(3), 155-174.

Shaikh, A. A., & Karjaluoto, H. (2015). Mobile banking adoption: A literature review. *Telematics and Informatics*, 32(1), 129–142. https://doi.org/10.1016/j.tele.2014.05.003

Sharma, R., Mehta, K., & Sharma, P. (2024). Role of artificial intelligence and machine learning in fraud detection and prevention. In *Risks and challenges of AI-driven finance: Bias, ethics, and security* (pp. 90–120). IGI Global.

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

Thekkethil, M. S., Shukla, V. K., Beena, F., & Chopra, A. (2021). Robotic Process Automation in Banking and Finance Sector for Loan Processing and Fraud Detection. *International Conference on Computer Communications*. https://doi.org/10.1109/ICRITO51393.2021.9596076

UiPath. (2022). *JPMorgan Chase leverages UiPath RPA to combat financial fraud*. Retrieved from https://www.uipath.com/resources/automation-case-studies/jpmorgan-chase

Venigandla, K., & Vemuri, N. (2022). RPA and AI-driven predictive analytics in banking for fraud detection. *Tuijin Jishu/Journal of Propulsion Technology*, *43*(4), 356. ISSN: 1001-4055.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478. https://doi.org/10.2307/30036540

Wilds, C. (2019). Examples of RPA in Banking Operations - Implementation in Lending. Retrieved from https://thelabconsulting.com/examples-rpabanking-operations-robotic-process-automation-implementation-commercial-lending/

Willcocks, L., & Lacity, M. (2016). *Service automation: Robots and the future of work*. Steve Brookes Publishing. Retrieved from University of Buckingham: https://www.buckingham.ac.uk/wp-content/uploads/2021/08/Service-Automation-Robots-and-the-Future-of-Work.pdf

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

Zhou, S., Jadoon, W., & Shuja, J. (2021). Machine learning-based offloading strategy for lightweight user mobile edge computing tasks. *Complexity*, 2021, 1-11.

윤일영. (2017). 로봇과 비즈니스의 융합, 로봇 프로세스 자동화(RPA). 융융합 Weekly TIP, 99 (2017 December), 1-10.