

Artificial Intelligence-Based Detection of Online Financial Fraud Using Machine Learning Techniques in Kenya

Sasha Siika*

Abstract

The increasing use of digitized financial services has significantly enhanced efficiency and convenience of online transactions. Conversely, the situation tends to simultaneously create opportunities for criminals to commit financial fraud. This study sought to examine application of AI in detection of online financial fraudulent activities in Kenya using machine learning techniques. Specific objectives comprised: to identify common patterns associated with online financial fraud in Kenya, assess the use of machine learning techniques in fraud detection, examine the effectiveness of AI in detecting online financial fraud, and recommend strategies for improving AI-driven fraud detection systems. Descriptive cross-sectional research design was used, allowing application of both quantitative and qualitative data. Target population included 54 respondents comprising fraud analysts, cybersecurity professionals, information technology officers, risk and compliance officers, and mobile money managers. Out of these respondents, 41 provided usable responses, accounting for a 75.9% response rate. Data was analyzed using frequencies, percentages, means, standard deviations, and one-sample t-tests against a neutral midpoint of 3.00. Phishing, social engineering, account takeover, identity theft, and exploitation of mobile money and digital payment platforms were found to be prominent fraud patterns. The findings further showed that although real-time integration and frequent model retraining remained comparatively underdeveloped, machine learning was reportedly being utilized more often to detect suspicious transactions and unusual customer behaviour. More than 70% agreed that AI-based fraud detection was successful, especially when it came to increasing detection speed and accuracy, identifying new fraud trends, and preventing fraud in general. The study concluded that AI and machine learning provide significant potential for strengthening online financial fraud detection in Kenya. It recommended enhanced investment in real-time AI systems, continuous model retraining, improved data infrastructure, staff capacity development, human-AI collaboration. Finally, the study recommended stronger regulatory and governance frameworks for responsible AI utilization.

Keywords: online financial fraud, AI, fraud detection, machine learning, digital financial systems



<https://doi.org/10.31039/ljss.2026.12.393>

* Student-Keny



1.0 Introduction

The rapid expansion of digital financial services has completely transformed the global financial ecosystem by improving the effectiveness, accessibility, and ease of financial transactions. Financial inclusion has expanded dramatically as a result of the growth of online banking, mobile money, digital wallets, e-commerce platforms, and real-time payment systems, but it has also given new opportunities to cybercriminals. Traditional identity theft and card fraud have given way to more complex online attacks involving phishing, account takeover, synthetic identities, authorized push payment fraud, malware, and cybercrime aided by artificial intelligence (AI). Conventional rule-based fraud detection systems are gradually unable to cope with the speed, complexity, and adaptive nature of modern financial crimes. As a result, machine learning (ML) in particular has become a potential solution that can detect anomalies in real time, uncover hidden fraud patterns, and continually learn from evolving fraud behaviours (Wang, 2023; Al-Obeidat et al., 2022).

Globally, online financial fraud continues to cause massive financial losses for organizations, consumers, governments, and financial institutions. According to Wang (2023), one of the most important issues facing digital finance is fraud protection since the exponential growth in digital financial transactions has increased the attack surface that fraudsters can exploit. In order to get over traditional security measures, modern fraud schemes increasingly include automated bots, social engineering, identity manipulation, and AI-generated false material. Machine learning algorithms can examine millions of transactions at once, identify minute behavioural abnormalities, and continuously update detection models as fraud trends evolve. This is in contrast to conventional detection techniques that rely on predetermined criteria.

In a comprehensive analysis of the literature on financial fraud detection, Al-Obeidat et al. (2022) discovered that supervised machine learning techniques consistently outperformed conventional statistical approaches in terms of fraud detection accuracy. Examples of these ML approaches include Random Forest, Decision Trees, Support Vector Machines, Artificial Neural Networks, and Gradient Boosting. The review also demonstrated that ensemble learning models typically achieved improved prediction performance because they successfully integrated various classification strategies to reduce false positives and enhance fraud identification.

Globally, concerns about consumer protection have increased due to the increasing sophistication of digital payment fraud. Ballaji (2024) contended that although digital payment systems have sped up economic expansion and financial inclusion, current legal and regulatory frameworks have found it difficult to keep up with new fraud tactics. Stronger AI-supported fraud monitoring systems and strong legislative protections are required since consumers are more vulnerable to identity theft, account compromise, unauthorized transactions, and data breaches. Similarly, Yang (2025) draws attention to the sharp increase in Authorized Push Payment (APP) fraud, in which victims are tricked into willingly sending money to con artists. The research further noted that without sophisticated AI systems that can identify questionable behavioural patterns prior to the finalization of transactions, compensation mechanisms by themselves are unable to effectively address the problem. According to Abdelhafez (2026), in the digital economy, consumer education is still crucial but insufficient. This is because fraud schemes are evolving more quickly than human



awareness, which highlights the need for intelligent fraud detection technologies that support consumer self-protection strategies.

Additionally, recent empirical research demonstrates how crucial consumer readiness is becoming in the fight against digital payment fraud. In their study on digital payment users in India, Lonkar et al. (2025) discovered that while adoption of digital payments had greatly increased, consumer awareness and readiness against online financial fraud remained insufficient. This left users vulnerable to phishing, fraudulent applications, and identity-related attacks. To improve financial security, the authors suggested integrating improved consumer awareness campaigns with machine learning-driven fraud detection. Similarly, Li and Chen (2025) created a dynamic machine learning anti-fraud model that uses continuously updated transaction behaviour to evaluate fraud risks in real-time. According to their research, dynamic machine learning models significantly outperformed static rule-based systems in terms of detection speed and accuracy. This allowed financial institutions to successfully respond to rapidly evolving fraud strategies.

In the context of regional Africa, mobile money innovations, agency banking, and fintech development have all contributed to the notable growth of digital financial services. However, escalating instances of electronic fraud that target financial institutions, Savings and Credit Cooperative Organizations (SACCOs), companies, and individual customers have coincided with increased digital financial inclusion. In many African financial institutions, the growing complexity of fraud schemes has revealed weaknesses in traditional fraud detection systems, especially in cases where fraud detection still mostly depends on manual assessments and pre-established regulations.

A systematic review of AI-driven fraud detection in SACCO transactions by Ampumuza et al. (2026) revealed that artificial intelligence is becoming more widely used in financial cooperative. This is because of its superior capacity to identify emerging fraud behaviours, reduce false alarms, and detect hidden transaction patterns. This review further noted that single-model approaches were less successful than hybrid machine learning models that integrated supervised and unsupervised learning techniques in identifying previously undiscovered fraud scenarios. However, the authors noted that a number of African financial institutions still face difficulties because of a lack of high-quality training data, insufficient technological know-how, poor model explainability, and a lack of regulations controlling the application of AI.

In Kenya, research indicates that financial institutions in Kenya have started to acknowledge artificial intelligence as a tactical instrument for enhancing their capacity to detect fraud. The Central Bank of Kenya (2025) reports that commercial banks have embraced AI applications in cybersecurity, fraud detection, risk management, customer service, and credit evaluation. This study further showed that institutional investment in AI technology is increasing, despite significant differences in implementation maturity amongst institutions. It also noted obstacles that continue to impede the widespread implementation of sophisticated AI-based fraud detection systems, such as inadequate AI governance frameworks, explainability concerns, data privacy concerns, skills shortages, and infrastructure constraints.

Despite growing regional and worldwide evidence in favour of AI-driven fraud detection, there are still significant knowledge gaps in the Kenyan environment. The majority of the



existing literature has focused on algorithm development, systematic reviews, legal perspectives, or institutional implementation. This has been the case without sufficiently analyzing the typical fraud patterns encountered in Kenya, the extent to which machine learning techniques are currently employed, their effectiveness in identifying online financial fraud, and useful strategies for enhancing AI-driven fraud detection systems. As fraud strategies continue to evolve with rapid digital financial innovation in Kenya's unique digital financial ecosystem, empirical data that combines fraud pattern analysis with machine learning applications and AI efficacy is required. Therefore, the current study examined application of AI in detection of online financial fraudulent activities in Kenya using machine learning techniques.

Specifically, the study sought to:

- i. To identify common patterns associated with online financial fraud in Kenya.
- ii. To assess the use of machine learning techniques in fraud detection.
- iii. To examine the effectiveness of AI in detecting online financial fraud.
- iv. To recommend strategies for improving AI-driven fraud detection systems

2.0 Theoretical Framework and Empirical Review

2.1 Theoretical Framework: Anomaly Detection Theory

The Anomaly Detection Theory, which serves as the foundation for numerous machine learning and artificial intelligence applications in fraud detection, provides a suitable theoretical framework for this investigation. Through their research on statistical outliers, Vic Barnett and Toby Lewis developed the theory, which was subsequently expanded in machine learning and data mining for anomaly identification (Barnett & Lewis, 1994). According to the theory, fraudulent activities can be detected by looking for anomalies in big datasets since they are uncommon occurrences that drastically depart from typical behavioural patterns. Anomaly detection algorithms establish a baseline of legitimate behaviour and identify unusual transactions or activities for additional research, as opposed to merely depending on pre-established norms. According to Chandola et al. (2009), this theoretical perspective is especially relevant in digital financial contexts because fraudsters constantly change their strategies, reducing the effectiveness of conventional rule-based detection systems.

This study is grounded in the Anomaly Detection Theory, which explains how machine learning algorithms based on artificial intelligence find common patterns of online financial crime in Kenya by continuously analyzing transactional data and behavioural abnormalities. It supports the first objective by enabling identification of unusual fraud patterns, the second objective by providing the conceptual basis for applying supervised, unsupervised, and hybrid machine learning algorithms in fraud detection, and the third objective by explaining how adaptive learning helps AI models achieve higher detection accuracy. The theory also contributes to the fourth objective by highlighting explainable AI, anomaly threshold optimization, continuous model training, and the integration of various data sources to enhance fraud detection performance. As a result, the theory presents a strong conceptual



framework for analyzing how well AI-driven fraud detection systems work in Kenya's rapidly evolving digital financial ecosystem (Barnett & Lewis, 1994; Chandola et al., 2009).

2.2 Empirical Literature Review

2.2.1 Common Patterns Associated with Online Financial Fraud

In order to investigate common fraud patterns and the effectiveness of fraud detection techniques in various banking environments, Phiri et al. (2024) compared online banking fraud cases in South Africa and Spain. Despite variations in institutional readiness and legislative responses, the study used comparative analysis to identify phishing attempts, identity theft, credential compromise, and unauthorized account access as the most common types of online banking fraud in both countries. The authors came to the conclusion that fraud patterns are becoming more complex and adaptable, necessitating constant observation and international information exchange. These results are consistent with Li et al. (2022), who contend that fraudsters increasingly operate through interconnected digital networks. However, they contrast with those of Mursi et al. (2025), whose research focuses on AI-enabled SMS scam detection in Kenya. Although Phiri et al. (2024) offer insightful cross-national comparisons, their study is constrained by its concentration on banking fraud in two countries. This leaves a contextual gap about the wider range of online financial fraud impacting Kenya's digital financial ecosystem, which the current study aimed to fill.

Cole (2023) conducted a critical analysis of online financial fraud rules in order to investigate how institutional practices in financial institutions may unintentionally encourage online fraud. The study discovered that the continuation of online financial crime is largely caused by insufficient governance structures, disjointed fraud reporting mechanisms, slow response systems, and an excessive dependence on client responsibility. The analysis argues that institution-wide risk governance backed by advanced detection technology should take precedence over customer awareness in the fight against fraud. These results differ from those of Li et al. (2022), who focus mostly on technology rather than organizational factors. However, they are consistent with Awuondo and Mutswenje (2025), who highlight governance weaknesses as major causes of fraud prevalence in Kenyan banks. In terms of methodology, Cole's policy evaluation is primarily conceptual and does not conduct an empirical analysis of the fraud patterns that users of the financial system encounter. The current study aimed to close the conceptual and empirical gaps on the specific fraud types that machine learning systems should prioritize in the Kenyan setting.

With its extensive use of internet banking, digital lending platforms, mobile money services, and electronic payment systems, Kenya is one of Africa's top digital financial economies. With millions of transactions carried out every day through mobile-based financial systems, the nation's leadership in digital banking has significantly improved financial inclusion. But at the same time, this rapid digital revolution has made people more vulnerable to sophisticated online financial fraud. In order to target individual and financial institutions, fraudsters are increasingly using phishing assaults, SIM swap fraud, social engineering, phony investment schemes, account takeovers, identity theft, and mobile banking vulnerabilities. Increased investment in AI-powered detection solutions is required because growing transaction volumes have made traditional fraud detection systems less efficient at spotting quickly changing fraud patterns.



Awuondo and Mutswenje (2025) examined the relationship between digital banking governance and fraud prevalence among Tier One banks in Mombasa County, Kenya. They found that weak cybersecurity procedures, insufficient fraud monitoring, and inadequate governance controls all significantly increased the number of fraud incidents. Equally, Mursi et al. (2025) showed that smishing, or SMS phishing, has emerged as one of Kenya's fastest-growing digital fraud patterns and created an AI model that is culturally sensitive and may enhance SMS scam detection by utilizing contextual and local language. Their results demonstrate the expanding role of AI in identifying sophisticated fraud networks. They complement those of Li et al. (2022), who suggested graph learning approaches for detecting intricate relationships among fraudulent transactions. Nevertheless, while Awuondo and Mutswenje (2025) focused mostly on governance and Mursi et al. (2025) concentrated on a single fraud type, neither study comprehensively investigated the diversity of online financial fraud patterns within Kenya's larger digital financial ecosystem. This contextual and conceptual gap justifies the current study's focus on identifying the common patterns associated with online financial fraud in Kenya before assessing AI-based detection approaches.

2.2.2 Use of Machine Learning Techniques in Fraud Detection

In their analysis of the use of machine learning algorithms in fraud detection, Olushola and Mart (2024) showed that supervised learning techniques perform better than traditional rule-based fraud detection systems by identifying hidden transaction patterns and adjusting to changing fraud behaviours. These include Decision Trees, Random Forest, Logistic Regression, and Support Vector Machines. According to the study, ensemble models are appropriate for large-scale financial transaction monitoring because they typically yielded higher predictive accuracy while reducing false positives. These findings are consistent with those of Almazroi and Ayub (2023), which showed better online payment fraud detection using machine learning models. Equally, Ali et al. (2022), in their systematic study identified Random Forest and Gradient Boosting as among the most effective fraud detection approaches. However, the current research aimed to address the methodological constraint regarding the applicability of these algorithms in emerging digital economies like Kenya, as Olushola and Mart (2024) mostly relied on publicly available benchmark information.

Gandhar et al. (2024) found that deep neural networks performed better in identifying intricate and previously undiscovered fraud patterns because of their capacity to learn high-dimensional representations of transaction data when compared to traditional machine learning methods for fraud detection. Similarly, Alam et al. (2025) demonstrated that adversarial machine learning improves the robustness of fraud detection by empowering models to resist attempts by cybercriminals to manipulate detection algorithms. This was especially the case in high-frequency financial transactions. The conclusions of Almazroi and Ayub (2023), who support hybrid machine learning frameworks for increasing fraud detection accuracy, are supported by these findings. However, Gandhar et al. (2024) and Alam et al. (2025) focused mainly on algorithmic performance under experimental conditions, paying little attention to implementation issues such as data quality, explainability, computational costs, and institutional preparedness. As a result, there is a practical and contextual gap in their research concerning the implementation of machine learning methods in Kenya's banking industry.



Through a comprehensive systematic literature review, Ali et al. (2022) synthesized global evidence on machine learning-based financial fraud detection and came to the conclusion that supervised learning is still the most popular approach. This is despite the growing potential of hybrid and unsupervised models for identifying new fraud patterns. The review stressed continuing issues relating to class imbalance, limited labeled datasets, feature engineering, and model interpretability. These findings align with those of Ijakaa and Kingi (2025), who discovered that machine learning and artificial intelligence have significant potential to prevent cybercrime in Kenya. However, they also noted that insufficient policy support, limited AI infrastructure, and insufficient technical capacity were the main obstacles to successful implementation. Although Ijakaa and Kingi (2025) concentrate on the education sector and Ali et al. (2022) offer extensive global evidence, neither study explicitly looked at the extent to which machine learning techniques are currently used in Kenya to detect online financial fraud. The current study, which aims to evaluate the application of machine learning algorithms in fraud detection in Kenya's digital financial environment, is based on this contextual and empirical gap.

2.2.3 Effectiveness of AI In Detecting Online Financial Fraud

According to Bello et al. (2023), who examined AI-driven approaches for real-time fraud detection in US financial transactions, artificial intelligence greatly improves fraud detection through automated anomaly detection, predictive analytics, and continuous transaction monitoring. According to the study, AI models increase institutional responses to new fraud threats by increasing detection speed while reducing false positives when compared to traditional rule-based systems. These results are in line with Bello and Olufemi (2024), who identify machine learning and deep learning as transformative technologies in fraud prevention. The same applies to Narender and Anand (2025), who argued that AI enables adaptive learning and real-time decision-making in financial fraud detection. However, the findings of Bello et al. (2023) may be applicable to developing economies like Kenya because they are situated within a fully digitalized financial environment with sophisticated AI infrastructure. Due to this contextual gap, an empirical assessment of AI effectiveness in Kenya's evolving digital financial landscape is required.

In their comprehensive analysis of artificial intelligence approaches used in fraud prevention, Bello and Olufemi (2024) came to the conclusion that machine learning, deep learning, natural language processing, and predictive analytics significantly increase the accuracy, scalability, and operational efficiency of fraud detection. However, the authors also noted persistent challenges that limit the application of AI, such as algorithmic bias, data privacy issues, explainability constraints, and integration costs. These results align with those of Bansal et al. (2025), which revealed that while AI is superior to manual fraud detection, the best outcomes are obtained when intelligent systems supplement human judgment rather than replacing it. Similarly, Narender and Anand (2025) support hybrid human-AI decision frameworks to improve transparency and trust. Despite these contributions, the reviewed research are still mostly conceptual and technology-focused, with few empirical data on the real effectiveness of AI systems used in African financial institutions. This is the gap the current study sought to fill.



In the African setting, Kunambura et al. (2026) examined the use of AI for bank fraud detection in Zimbabwe and found that it greatly enhances risk management, operational effectiveness, and fraud identification. However, insufficient financial resources, poor data quality, regulatory ambiguity, and a lack of technical competence all hindered adoption. Mursi et al. (2025) revealed similar findings, demonstrated the promise of AI in addressing localized cyber fraud. Their culturally tailored AI model successfully identified smishing attacks in Kenya by incorporating local linguistic and contextual factors.

Although these studies support AI's effectiveness in combating specific forms of fraud, their scope varies. While Mursi et al. (2025) concentrated on SMS fraud detection, Kunambura et al. (2026) investigated organizational adoption. The overall effectiveness of AI in identifying various types of online financial fraud throughout Kenya's digital financial ecosystem is not thoroughly assessed in either study. The current study is based on filling this conceptual and contextual gap.

Furthermore, Kiula (2026) points out that operational cybersecurity issues still exist even though machine learning models have greatly enhanced fraud detection performance in Kenya's financial industry. The study highlights that adversarial assaults that might manipulate fraud detection outcomes may target machine learning systems themselves. The study demonstrated that secure machine learning model deployment necessitates continuous monitoring, model explainability, cybersecurity integration, and strong governance. This allows the process to preserve trust and effectiveness in fraud detection systems using the STRIDE cybersecurity framework, explainable AI techniques, and anomaly gating mechanisms. These findings further prove that effective AI implementation encompasses operational resilience and cybersecurity readiness in addition to prediction accuracy.

3.0 Research Methodology

Descriptive cross-sectional research design was adopted in the study, allowing triangulation of both quantitative and qualitative data for a more comprehensive analysis. Target population for the study comprised fraud analysts, cybersecurity professionals, information technology officers, risk and compliance officers, and mobile money managers. These were randomly identified from selected commercial banks, fintech companies, mobile money service providers, and relevant financial regulatory institutions in Kenya. Initially, 62 of these were identified, before a sample size of 54 respondents was selected using the Yamane (1967) statistical formula (at a 95% confidence level and a 5% margin of error). Stratified random sampling approach was used to ensure fair representation across the different institutions and professional categories, as illustrated below.

$$n = \frac{N}{1+N(e)^2}$$

Where:

n = sample size

N = population size (62)

e = margin of error (0.05 at 95% confidence level)



$$n = \frac{62}{1+62(0.05)^2} = \frac{62}{1+0.155} = \frac{62}{1.155} \approx 54$$

Table 3.1 Sample Size

Stratum	Target Population (N)	Percentage (%)	Sample Size (n)
Fraud Analysts	13	21.0	11
Cybersecurity Professionals	12	19.4	10
Information Technology Officers	15	24.2	13
Risk and Compliance Officers	12	19.4	10
Mobile Money Managers	10	16.0	9
Total	62	100	54

Primary data was collected using a structured self-administered questionnaire comprising closed-ended Likert-scale items and a few open-ended questions to capture detailed information representing the respondents' views. Quantitative data was analyzed using descriptive statistics (frequencies, percentages) and inferential statistics (correlation and multiple regression analysis), where SPSS computer software was used for the analysis.

4.0 Research Findings

4.1 Background Information of the Respondents

Out of the sample size of 54, the study managed to have 41 questionnaires fully completed and returned, making a response rate of 75.9%. There was a representative distribution across the five professional strata as illustrated in table 4.1.

Table 4.1 Respondents' Background Information

Background characteristic	Category	Frequency (f)	Percentage (%)
Professional category	Fraud Analyst	8	19.5
	Cybersecurity Professional	8	19.5
	Information Technology Officer	10	24.4
	Risk and Compliance Officer	8	19.5
	Mobile Money Manager	7	17.1
	Total	41	100.0
Gender	Male	25	61.0
	Female	16	39.0
	Total	41	100.0
Age	Below 25 years	2	4.9
	25–34 years	13	31.7



	35–44 years	16	39.0
	45–54 years	8	19.5
	55 years and above	2	4.9
	Total	41	100.0
Highest level of education	Diploma	3	7.3
	Bachelor's degree	18	43.9
	Master's degree	17	41.5
	Doctorate	2	4.9
	Other	1	2.4
	Total	41	100.0
Years of professional experience	Less than 3 years	5	12.2
	3–5 years	10	24.4
	6–10 years	15	36.6
	11–15 years	7	17.1
	More than 15 years	4	9.8
	Total	41	100.0
Type of organization	Commercial Bank	14	34.1
	Fintech Company	9	22.0
	Mobile Money Service Provider	10	24.4
	Financial Regulatory Institution	5	12.2
	Other	3	7.3
	Total	41	100.0
Experience with fraud detection technologies	None	2	4.9
	Less than 2 years	6	14.6
	2–5 years	13	31.7
	6–10 years	14	34.1
	More than 10 years	6	14.6
	Total	41	100.0

The tabulated results show that respondents were fairly evenly distributed among the professional categories, with Information Technology Officers making up the largest group (24.4%), followed by Fraud Analysts, Cybersecurity Professionals, and Risk and Compliance Officers (19.5% each), and Mobile Money Managers (17.1%). Because the study needed the opinions of experts who are actively and directly involved in technology, fraud control, compliance, and digital financial services, this distribution is appropriate. Males were more prevalent (61.0%) than females (39.0%) in the gender distribution, which reflects the historically male-dominated nature of technical and cybersecurity-related industries, while still providing significant female representation.



The age distribution shows that 70.7% of respondents were between the ages of 25 and 44, with the majority (39.0%) being between 35 and 44 years, and 25-34 years (31.7%). This suggested that the majority of the respondents belonged to the both technologically savvy and economically active workforce. In terms of education, 85.4% of respondents had either a bachelor's degree (43.9%) or a master's degree (41.5%), indicating that they were reasonably well-educated and able to provide knowledgeable evaluations of AI and machine learning applications. Similarly, 82.9% had at least two years of expertise with fraud detection technology, and 63.4% had at least six years of professional experience. This is especially significant since it implies that the majority of respondents had adequate professional and technological experience to offer reliable information about machine learning applications, online financial fraud trends, and the effectiveness of AI-based detection systems.

With respondents predominantly from commercial banks (34.1%), mobile money providers (24.4%), and fintech organizations (22.0%), the organizational distribution also demonstrates useful contextual diversity. Collectively, these institutions account for 80.5% of the respondents and represent key components of Kenya's digital financial ecosystem. Nevertheless, the relatively small percentage (12.2%) of regulatory organizations provides a critical supervisory perspective. Overall, the background distribution indicates that the 41 respondents are a professionally relevant and adequately experienced group for investigating AI-based online financial fraud detection in Kenya. Additionally, the 75.9% response rate was sufficient enough to anchor a strong analysis of the three study objectives.

4.2 Common Patterns Associated with Online Financial Fraud

The first study objective was to identify common patterns associated with online financial fraud in Kenya. A 5-points (SD=strongly disagree, D=disagree, N=neutral, A=agree, SA=strongly agree) Likert scale was used to test different items, with inferential statistics applied to show the level of correlations among the variables of the study. Table 4.2 provides a summary of the findings.

Table 4.2 Common Patterns Associated with Online Financial Fraud (N=41)

Statement	SD (%)	D (%)	N (%)	A (%)	SA (%)	Mean	SD	t-value	p-value
B1. Phishing and deceptive messages are common methods used to obtain customers' financial information.	2 (4.9)	3 (7.3)	4 (9.8)	15 (36.6)	17 (41.5)	4.02	1.13	5.81	<.001
B2. Social engineering is frequently used to manipulate customers into authorizing fraudulent transactions.	2 (4.9)	4 (9.8)	6 (14.6)	16 (39.0)	13 (31.7)	3.83	1.14	4.67	<.001



B3. Account takeover and identity theft are common forms of online financial fraud.	1 (2.4)	3 (7.3)	5 (12.2)	17 (41.5)	15 (36.6)	4.02	1.01	6.48	<.001
B4. Fraudsters commonly use mobile money and digital payment platforms to conduct fraudulent transactions.	1 (2.4)	3 (7.3)	6 (14.6)	16 (39.0)	15 (36.6)	4.00	1.02	6.25	<.001
B5. Online financial fraud patterns are becoming increasingly sophisticated and difficult to detect using conventional methods.	0 (0.0)	2 (4.9)	4 (9.8)	15 (36.6)	20 (48.8)	4.29	0.84	9.81	<.001
Overall Objective 1	—	—	—	—	—	4.03	1.04	14.30	<.001

The results show that there is a strong perception that the identified forms of fraud are typical in Kenya. With 78.1% of respondents agreeing or strongly agreeing (Mean = 4.02), phishing and misleading mails earned high levels of agreement. Similarly, 78.1% agreed that identity theft and account takeover are frequent (Mean = 4.02), while 75.6% recognized digital payment platforms and mobile money as frequently exploited channels (Mean = 4.00). The agreement rate for social engineering was 70.7% (Mean = 3.83), which was relatively lower but still significant.

The strongest finding involved the growing sophistication of financial crime committed online. The study revealed that 85.4% of respondents agreed or strongly agreed that fraud patterns are getting more complex and challenging to identify with traditional techniques (Mean = 4.29). This is especially crucial for the current study since it supports the need to investigate AI and machine learning-based approaches that can identify evolving and previously unseen fraud trends.

The descriptive results were supported by the inferential statistics. With $p < .001$ in each instance, all five items produced statistically significant positive deviations from the neutral midpoint. Additionally, the neutral value, $t(204) = 14.30$, $p < .001$, was significantly lower than the total objective mean of 4.03. Therefore, the findings would corroborate the conclusion that respondents consider phishing, social engineering, identity theft/account takeover, exploitation of digital payment platforms, and increasingly complex fraud techniques as important patterns of online financial fraud.

Overall, examining whether machine learning techniques are being used to identify these patterns, and whether AI-based systems are effective in detecting them is justified by the high rating for increasingly sophisticated fraud. This implies that traditional rule-based approaches may be insufficient. The results also suggest that phishing, identity/account takeover,



mobile-money fraud, and social engineering should be given special attention as priority fraud patterns in subsequent analyses.

4.3 Use of Machine Learning Techniques in Fraud Detection

The second objective of the study was to assess the use of machine learning techniques in fraud detection. A 5-points (SD=strongly disagree, D=disagree, N=neutral, A=agree, SA=strongly agree) Likert scale was used to test different items, while inferential statistics was applied to demonstrate how the study variables were correlated. Table 4.3 presents a summary of the findings.

Table 4.3 Use of Machine Learning Techniques in Fraud Detection (N=41)

Statement	SD (%)	D (%)	N (%)	A (%)	SA (%)	Mean	SD	t-value	p-value
C1. Our organization uses machine learning techniques to detect suspicious financial transactions.	2 (4.9)	3 (7.3)	5 (12.2)	17 (41.5)	14 (34.1)	3.93	1.10	5.42	<.001
C2. Machine learning is used to identify unusual transaction and customer behaviour.	1 (2.4)	3 (7.3)	5 (12.2)	18 (43.9)	14 (34.1)	4.00	0.99	6.47	<.001
C3. Machine learning models are used to monitor financial transactions in real time.	3 (7.3)	5 (12.2)	7 (17.1)	15 (36.6)	11 (26.8)	3.63	1.20	3.37	.002
C4. Machine learning techniques are integrated with existing fraud detection and cybersecurity systems.	2 (4.9)	5 (12.2)	7 (17.1)	16 (39.0)	11 (26.8)	3.71	1.12	4.07	<.001
C5. Our organization regularly updates or retrains machine learning models to respond to emerging fraud patterns.	3 (7.3)	6 (14.6)	8 (19.5)	14 (34.1)	10 (24.4)	3.54	1.21	2.87	.006
Overall Objective 2	—	—	—	—	—	3.76	1.12	8.90	<.001



The findings demonstrate a generally positive perception on the application of machine learning techniques in fraud detection. With a mean score of 3.93 for C1, 75.6% of respondents agreed or strongly agreed that their organizations employ machine learning to identify questionable financial transactions. Also, 78.0% agreed or strongly agreed that machine learning is utilized to identify odd client behaviour and transactions (Mean = 4.00). This was the highest-rated application, and implied that behavioural and transaction irregularity identification represents one of the more established uses of machine learning in fraud detection.

At the same time, 63.4% of respondents agreed or strongly agreed with the use of machine learning for real-time transaction monitoring (Mean = 3.63). Similarly, 65.8% of respondents agreed that machine learning is integrated with current cybersecurity and fraud detection systems (Mean = 3.71). The comparatively lower ratings would suggest that despite the fact that organizations are implementing machine learning, complete integration with real-time operational systems is still a challenge. This could be related to data availability, system compatibility, expense, technological infrastructure, or a lack of specialized technical expertise.

While the majority (58.5%) still agreed or strongly agreed (Mean = 3.54), item C5, which dealt with the frequent updating or retraining of machine learning models, had the lowest rating. This revelation is significant because fraud trends are continuously evolving. This further means that a machine learning model that is not routinely retrained may eventually lose its effectiveness. The comparatively high neutral response of 19.5% could also be a sign of disparities in institutional awareness or implementation maturity, as some respondents are unsure whether their organizations routinely retrain models.

According to the inferential findings, all the five assertions were considerably above the neutral midpoint of 3.00. As demonstrated in the table, C1 produced $t = 5.42$, $p < .001$; C2 produced $t = 6.47$, $p < .001$; C3 produced $t = 3.37$, $p = .002$; C4 produced $t = 4.07$, $p < .001$; and C5 produced $t = 2.87$, $p = .006$. Thus, across all five dimensions, respondents' opinions about the application of machine learning techniques were notably positive.

Overall, the neutral midpoint ($t = 8.90$, $p < .001$) was considerably lower than the Objective 2 mean of 3.76. The conclusion that machine learning techniques are being applied in fraud detection among the institutions involved in the study is thus supported by the findings. This is especially the case when it comes to identifying unusual transaction and customer behavior and detecting suspicious transactions. However, the relatively lower ratings for frequent model retraining and real-time monitoring suggest that acceptance does not always equate to sophisticated or comprehensive implementation.

The findings indicate that fraud detection enabled by AI/ML is becoming more prevalent in Kenya's banking industry. However, implementation appears to vary depending on the function. Because skilled fraudsters constantly modify their techniques, the comparatively lower ratings for model retraining and real-time monitoring are especially significant. Strategies integrating continuous model training, enhanced data infrastructure, system integration, technical capacity development, and more robust AI governance are also suggested.



4.4 Effectiveness of AI in Detecting Online Financial Fraud

The third objective of the study was to examine the effectiveness of AI in detecting online financial fraud. A 5-points (SD=strongly disagree, D=disagree, N=neutral, A=agree, SA=strongly agree) Likert scale was used to test 5 different statements, while inferential statistics was applied to demonstrate the level of correlations between the study variables. Table 4.4 illustrates a summary of the findings.

Table 4.4 Effectiveness of AI in Detecting Online Financial Fraud (N=41)

Statement	SD (%)	D (%)	N (%)	A (%)	SA (%)	Mean	SD	t-value	p-value
D1. AI-based systems detect fraudulent transactions more accurately than conventional detection methods.	1 (2.4)	3 (7.3)	5 (12.2)	18 (43.9)	14 (34.1)	4.00	0.99	6.47	<.001
D2. AI enables faster identification and response to suspicious financial transactions.	1 (2.4)	2 (4.9)	4 (9.8)	18 (43.9)	16 (39.0)	4.12	0.95	7.58	<.001
D3. AI-based fraud detection systems reduce false alerts while identifying genuine fraudulent transactions.	2 (4.9)	4 (9.8)	6 (14.6)	17 (41.5)	12 (29.3)	3.80	1.10	4.66	<.001
D4. AI systems are effective in identifying new and previously unknown fraud patterns.	1 (2.4)	3 (7.3)	7 (17.1)	17 (41.5)	13 (31.7)	3.93	1.00	5.96	<.001
D5. Overall, AI-based fraud detection has improved the organization's ability to prevent online financial fraud.	1 (2.4)	3 (7.3)	5 (12.2)	17 (41.5)	15 (36.6)	4.02	1.01	6.48	<.001
Overall Objective 3	—	—	—	—	—	3.97	1.01	12.14	<.001

The findings indicated that most respondents considered AI-based solutions as effective at identifying online financial fraud. A mean score of 4.00 was obtained for D1, where 78.0% of respondents agreed or strongly agreed that AI-based solutions detect fraudulent transactions



more accurately than traditional approaches. D2 received the strongest response, with 82.9% agreeing or strongly agreeing that AI enables faster identification and quicker responding to questionable transactions (Mean = 4.12). This implies that the primary apparent benefit of AI is its capacity to quickly evaluate massive amounts of financial transactions and identify questionable activity almost instantly.

About the ability to reduce false alerts, 70.8% of respondents agreed or strongly agreed that AI-based solutions may identify real fraudulent transactions while reducing false alerts (Mean = 3.80). Despite being the lowest-rated effectiveness assessment, this evaluation is nonetheless positive. This suggests that even in situations where AI technologies are used, false positives continue to be a practical problem. Similarly, 73.2% of respondents agreed or strongly agreed that AI can identify genuine and unidentified fraud trends (Mean = 3.93). This is especially crucial because modern online financial fraud is becoming more sophisticated and may entail trends that are challenging to identify with static, rule-based systems.

Additionally, there was considerable support for AI's overall role in preventing fraud. According to 78.1% of respondents who agreed or strongly agreed (Mean = 4.02), the ability of their organization to avoid online financial crime has improved as a result of AI-based fraud detection. According to the distribution, respondents saw AI as an increasingly significant part of institutional fraud prevention and cybersecurity measures rather than just as a technology addition.

On the inferential findings, the one-sample t-test demonstrates that all five effectiveness indicators were significantly higher than the neutral midpoint of 3.00. D1 produced $t = 6.47$, $p < .001$; D2 produced $t = 7.58$, $p < .001$; D3 produced $t = 4.66$, $p < .001$; D4 produced $t = 5.96$, $p < .001$; and D5 produced $t = 6.48$, $p < .001$. Therefore, there is statistically significant evidence that respondents consider AI as effective across all the assessed dimensions.

Overall, the mean score for objective 3 was 3.97, which was much higher than the neutral value of 3.00 ($t = 12.14$, $p < .001$). The results corroborate the conclusion that, among the organizations represented by the respondents, AI-based technologies are perceived effective in detecting and preventing online financial fraud.

The results provide empirical support for the claim that AI can improve online financial fraud detection through increased speed, improved accuracy, identification of emerging fraud patterns, and enhanced prevention capabilities. However, the relatively lower score for reducing false alerts (Mean = 3.80) shows that AI effectiveness is not absolute. Factors like data quality, algorithmic bias, model training, explainability, system integration, and the evolving behaviour of fraudsters may affect performance. As a result, while the findings support the effectiveness of AI, human oversight, high-quality data, and institutional capacity building to optimize AI's contribution to fraud detection in Kenya.

5.0 Conclusions and Recommendations

5.1 Conclusions

The study came to the conclusion that online financial fraud in Kenya is characterized by increasingly sophisticated patterns. These include phishing, social engineering, account



takeover, identity theft, and exploitation of mobile money and digital payment platforms. It was further concluded that machine learning techniques are increasingly being applied to identify suspicious transactions and unusual customer behaviour. However, real-time integration and regular model retraining are areas that still require significant improvement. Overall, it was noted that AI-based fraud detection is effective, especially in improving detection swiftness, accuracy, identification of emerging fraud patterns, and overall fraud prevention.

5.2 Recommendations

Based on the study findings, Kenyan financial institutions should increase their investment in AI and machine learning-based fraud detection systems. In addition to integrating AI with current cybersecurity systems and developing staff capability in machine learning, cybersecurity, and AI governance, Kenyan institutions should routinely retrain and test models using current fraud data. To guarantee that AI-driven fraud detection is precise, safe, transparent, and adaptable to new fraud strategies, Kenyan financial institutions and regulators should also strengthen data-sharing channels, consumer awareness, explainable AI practices, and regulatory frameworks.



References

- Abdelhafez, S. (2026). Consumer Self-Protection Against Fraud in the Digital Economy: Strategies for Everyday Financial and Commercial Transactions. *Available at SSRN* 6704878.
- Alam, M. K., Mahmud, M. A., & ALAM, M. A. (2025). Adversarial Machine Learning for Robust Fraud Detection in High-Frequency Financial Transactions. *Journal of Computer Science and Technology Studies*, 7(8), 314-335.
- Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., ... & Saif, A. (2022). Financial fraud detection based on machine learning: a systematic literature review. *Applied Sciences*, 12(19), 9637.
- Almazroi, A. A., & Ayub, N. (2023). Online payment fraud detection model using machine learning techniques. *Ieee Access*, 11, 137188-137203.
- Al-Obeidat, F., Ali, S., Abdullah, M., Alotaibi, F., Althobaiti, T., & Alghamdi, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences*, 12(19), 9637. <https://doi.org/10.3390/app12199637>
- Ampumuza, D., Katushabe, C., & Tamale, M. (2026). A systematic review and future directions for AI-driven detection of fraud patterns in SACCO transactions. *Frontiers in Artificial Intelligence*, 8, 1690482.
- Awuondo, B. A., & Mutswenje, V. S. (2025). Digital banking governance and fraud prevalence in tier one banks in Mombasa County, Kenya. *International Academic Journal of Economics and Finance (IAJEF)* | ISSN 2518-2366, 5(2), 46-62.
- Ballaji, N. (2024). Consumer protection in the era of digital payments: legal challenges and solutions. *Beijing L. Rev.*, 15, 1268.
- Bansal, K., Paliwal, A. C., & Singh, A. K. (2025). Analysis of the benefits of artificial intelligence and human personality study on online fraud detection. *International Journal of Law and Management*, 67(2), 191-209.
- Barnett, V., & Lewis, T. (1994). *Outliers in statistical data* (3rd ed.). John Wiley & Sons.
- Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer science & IT research journal*, 5(6), 1505-1520.
- Bello, O. A., Ogundipe, A., Mohammed, D., Adebola, F., & Alonge, O. A. (2023). AI-driven approaches for real-time fraud detection in US financial transactions: Challenges and opportunities. *European Journal of Computer Science and Information Technology*, 11(6), 84-102.
- Central Bank of Kenya. (2025). *Survey on artificial intelligence in the Kenyan banking sector*. Central Bank of Kenya. Retrieved from [Central Bank of Kenya Survey on Artificial Intelligence in the Banking Sector](#)
- Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), 15. <https://doi.org/10.1145/1541880.1541882>
- Cole, T. (2023). How are financial institutions enabling online fraud? A developmental online financial fraud policy review. *Journal of Financial Crime*, 30(6), 1458-1473.



- Gandhar, A., Gupta, K., Pandey, A. K., & Raj, D. (2024). Fraud detection using machine learning and deep learning. *SN Computer Science*, 5(5), 453.
- Ijaka, J. B., & Kingi, P. M. (2025). Preventing Cybercrime through Artificial Intelligence and Machine Learning in Education, Kenya. *Journal of the Kenya National Commission for UNESCO*.
- Kiula, B. M. (2026). Operational security assessment of machine learning fraud detection systems: A cybersecurity perspective using STRIDE, explainability, and anomaly gating. *Science Discovery Artificial Intelligence*, 1(1). Retrieved from [Science Discovery Artificial Intelligence Article](#)
- Kunambura, M., Mugari, I., Nyakurimwa, C., & Nduku, C. (2026). Artificial intelligence (AI) adoption for bank fraud detection and prevention in Zimbabwe: Applications, adoption factors and policy implications. *African Journal of Computing, Data Science and Informatics*, 2(1), 33-65.
- Li, F., & Chen, Z. (2025). Dynamic quantification anti-fraud machine learning model for real-time transaction fraud detection in banking. *Discover Computing*, 28(59). <https://doi.org/10.1007/s10791-025-09549-7>
- Li, R., Liu, Z., Ma, Y., Yang, D., & Sun, S. (2022). Internet financial fraud detection based on graph learning. *IEEE Transactions on Computational Social Systems*, 10(3), 1394-1401.
- Lonkar, A., Dharmadhikari, S., Dharurkar, N., Patil, K., & Phadke, R. A. (2025). Tackling digital payment frauds: a study of consumer preparedness in India. *Journal of Financial Crime*, 32(2), 257-278.
- Mursi, J. K. A., Mwarika, S., Nach, H., Bukusi, N., Musomba, A., Murimi, W., & Kiboi, M. (2025, October). AI Against Smishing in Kenya: Culturally Adapted SMS Scam Detection for Digital Trust. In *2025 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD)* (pp. 1-8). IEEE.
- Narender, M., & Anand, A. J. (2025). Artificial intelligence in financial fraud detection. In *Handbook of AI-driven threat detection and prevention* (pp. 193-207). CRC Press.
- Olushola, A., & Mart, J. (2024). Fraud detection using machine learning. ScienceOpen Preprints.
- Phiri, J., Lavhengwa, T., & Segooa, M. A. (2024). Online banking fraud detection: A comparative study of cases from South Africa and Spain. *South African Journal of Information Management*, 26(1), 1-8.
- Wang, C. (2023). Overview of digital finance anti-fraud. In *Anti-Fraud Engineering for Digital Finance: Behavioral Modeling Paradigm* (pp. 1-10). Singapore: Springer Nature Singapore.
- Yamane, T. (1967). *Statistics: An introductory analysis* (2nd ed.). Harper & Row.
- Yang, C. (2025). Protecting financial consumers from authorized push payment fraud: is reimbursement an optimal solution? *Journal of Financial Regulation and Compliance*, 33(4), 642-653.

