

ADFJ ISSN 2522 – 3186.

African Development Finance Journal

VOLUME 9 (III)

*Application of Artificial Intelligence on Fraud Detection
and Prevention in Deposit Taking Savings and Credit
Cooperative Societies in Kenya*

Janice Ndegwa

Dr. Helen Wairimu Kinyua

Date Received: April 20, 2026

Date Published: September 03, 2026

Application of Artificial Intelligence on Fraud Detection and Prevention in Deposit Taking Savings and Credit Cooperative Societies in Kenya

By: Janice NDEGWA¹ and Helen Wairimu KINYUA (PhD)²

Abstract

Fraud remains a significant challenge for deposit-taking SACCOs, threatening financial sustainability and stakeholder trust. The increasing adoption of artificial intelligence presents an opportunity to strengthen fraud detection and prevention mechanisms. This study aimed to determine the effect of AI on fraud detection and prevention in deposit-taking SACCOs in Kenya. Anchored on the Technology Acceptance Model and Fraud Triangle Theory, it examined how AI implementation level, system complexity, employee training on systems, and regulatory compliance influenced fraud detection and prevention. It employed a descriptive research design targeting all 176 licensed deposit-taking SACCOs in Kenya, achieving a response rate of 62.5%. Primary data was collected through structured questionnaires to Chief Information Officers or Heads of IT. Descriptive statistics, correlation analysis, and multiple regression analysis were conducted using SPSS version 27. The regression model showed a strong explanatory power, with an R Square of 0.928, indicating that 92.8% of the variance in fraud detection and prevention is explained by independent variables. The results revealed that regulatory compliance had the strongest positive influence on fraud detection and prevention ($\beta = 0.739$, $p = 0.000$), followed by AI implementation level ($\beta = 0.349$, $p = 0.000$), system complexity ($\beta = 0.308$, $p = 0.000$), and employee training ($\beta = 0.227$, $p = 0.001$). These highlight the importance of aligning AI systems with regulatory standards, investing in robust implementation, and equipping employees with skills to operate AI technologies effectively. The study concludes that AI significantly enhances fraud detection and prevention in SACCOs, with regulatory compliance playing a critical role in ensuring the effectiveness of AI systems. SACCOs with higher levels of AI implementation and employee training, reported superior fraud management outcomes; it recommends that policymakers develop supportive frameworks for AI adoption, SACCOs prioritize continuous training and integration of AI technologies, and regulatory bodies enforce compliance standards to enhance fraud detection systems. Future research could explore the long-term impact of AI on fraud detection through longitudinal studies or expand the scope to include other financial institutions. Additionally, studies on emerging AI technologies, such as machine learning and blockchain, and their ethical implications would enrich the understanding of advanced fraud prevention systems.

Keywords: Artificial intelligence, fraud detection and prevention, deposit-taking SACCOs, financial technology, regulatory compliance, employee competency.

¹Faculty of Business and Management Sciences, University of Nairobi, Email: janicendegwa@gmail.com, ORCID: 0009-0004-2078-8058

² Senior Lecturer, Department of Finance and Accounting, Faculty of Business and Management Sciences, University of Nairobi, Email: helen.kinyua@uonbi.ac.ke, ORCID: 0009-0004-4598-6157

1. INTRODUCTION

The relationship between artificial intelligence (AI) and fraud detection and prevention is fundamentally transformative. AI technologies, through their data analysis capabilities, can enhance the accuracy and efficiency of detecting fraudulent activities (Bello & Olufemi, 2024). As per Gupta, (2024), the level of AI implementation, including the sophistication of systems and the quality of employee training, directly influences how effectively these technologies can identify and respond to potential fraud. Complex systems equipped with machine learning algorithms can analyze vast amounts of data in real time, identifying patterns and anomalies that might indicate fraudulent behavior (Zayed et al., 2024). Well-trained employees can leverage AI tools more effectively, ensuring timely and accurate responses to fraud incidents (Romero et al., 2024).

Artificial intelligence involves the simulation of the various human intelligence processes, (Gupta, 2024; Kok & Siripipatthanakul, 2023). It focuses on creating intelligent agents that interact with their environment to achieve specific goals (Adelakun et al., 2024). Researchers have operationalized AI in different ways, such as measuring the extent of technology adoption, like the number and sophistication of AI tools used in an organization (Nguyen et al., 2021), assessing improvements in efficiency and decision-making quality (Issa et al., 2022), and evaluating user interaction factors (Kelly et al., 2023).

Empirical research on artificial intelligence (AI) demonstrates its significant influence across industries. In manufacturing, AI adoption has improved productivity by 20% through automation and enhanced quality control (Dhameliya, 2023). In finance, AI-driven systems increased risk assessment accuracy by 30%, leading to more strategic investments and lower default rates (Batchu, 2023). In healthcare, diagnostic AI tools reduced errors by 25%, improving patient outcomes (Alowais et al., 2023). Service-oriented firms reported a 15% rise in customer satisfaction due to personalized interactions (Hsu & Lin, 2023). However, concerns persist over potential job displacement, although AI also promotes workforce up-skilling (Nazareno& Schiff, 2022). These findings underscore AI's transformative potential in boosting efficiency, decision-making, and customer experience while presenting ethical and employment challenges.

1.1 Research Problem

Conceptually the integration of AI in fraud detection and prevention has become an important organization security measure. AI has can revolutionize how organizations identify and mitigate fraudulent activities (Bello &Olufemi, 2024). The relationship between AI implementation level, system complexity, and employee training presents a compelling research focus. Studies suggest that the effectiveness of AI in fraud prevention depends on the presence of AI systems and their sophistication and employee training (Gupta, 2024). However, Ahmed et al. (2022) argue that highly complex AI models enhance performance in tasks like fraud detection due to their ability to process vast datasets and uncover hidden patterns. Zakaria et al. (2023) argue that highly complex AI systems are essential for effective fraud detection; while others caution that over-reliance on such systems oversight could reduce effectiveness.

Scholars such as Gupta (2024) emphasize that the success of AI in mitigating fraud depends on deploying AI technologies and their sophistication and the competence of employees using them. Conversely, Ahmed et al. (2022) poses that complex AI models like deep learning significantly improve performance in fraud detection. Yet, Zakaria et al. (2023) warn that overreliance on complex AI systems without adequate human oversight may reduce overall effectiveness. Hence, there exists a research gap in understanding how varying degrees of AI implementation, system sophistication, and user readiness jointly affect fraud prevention, particularly in the context of Kenya's deposit-taking SACCOs.

2. METHODS

A descriptive research design targeting all 176 licensed deposit-taking SACCOs in Kenya was adopted by the study. The respondents included Chief Information Officers and Heads of Information Technology within the SACCOs.

Structured questionnaires were used to collect primary data; this achieved a response rate of 62.5%. The independent variables were, AI implementation level, AI system complexity, Employee training on AI systems and Regulatory compliance, while the dependent variable was fraud detection and prevention.

2.1. Literature Review

2.1.1. Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM), developed by Davis (1989), provides a theoretical lens to understanding the determinants of technology adoption. It asserts that two perceptions—usefulness and ease of use—shape individuals’ attitudes toward technology, which then influence their intention and actual use. Although TAM has been extensively applied across disciplines, it faces criticism for being overly simplistic. It often neglects contextual and organizational factors such as infrastructure, social influence, and support systems. Its deterministic nature assumes that perceived usefulness automatically translates into adoption, ignoring situations where institutional or regulatory barriers exist. Furthermore, it overlooks how user perceptions evolve over time with continued exposure to technology. For this study, TAM is relevant in explaining how SACCO employees perceive and adopt AI technologies. The level of AI implementation, its complexity, and the adequacy of training can affect employees’ perceptions of usefulness and ease of use. By employing TAM, the study identifies enablers and barriers influencing AI adoption for fraud prevention in SACCOs.

2.1.2. Fraud Triangle Theory

The Fraud Triangle Theory, introduced by Donald Cressey (1953), remains foundational in explaining why individuals commit fraud. It identifies three essential elements: pressure, opportunity, and rationalization. The theory suggests that reducing any of these three factors lowers the likelihood of fraud occurrence. However, the model has been critiqued for emphasizing individual behavior while underplaying systemic or organizational influences. In the context of AI-driven fraud prevention, the theory offers a useful analytical framework. AI can reduce opportunity by automating internal controls, enhancing real-time transaction monitoring, and identifying anomalies quickly. It can detect behavioral trends linked to pressure or rationalization by analyzing user behavior and access patterns.

2.2. Empirical Review

Numerous empirical studies have explored AI’s influence on fraud detection across diverse contexts. Kotagiri (2023) examined the impact of AI integration in U.S. banks using a survey of IT and compliance officers and found a strong positive relationship between AI implementation

and fraud prevention effectiveness. Mohanty and Mishra (2023) investigated AI's role in Indian financial institutions, emphasizing system complexity and employee training, and found that well-trained staff and sophisticated AI systems significantly improved fraud prevention. Martínez et al. (2022) conducted a similar study in European banks and found that AI implementation, complexity, and training positively affected fraud prevention. Găbudeanu et al. (2021) studied AI's impact on Spanish institutions and found similar results. Zhu et al. (2021) in China also reported that AI adoption enhances fraud prevention outcomes. In Kenya, Mwavali (2024) found that AI implementation, system complexity, and training positively influenced fraud detection in commercial banks. Millan and Ibua (2023) conducted a literature review on AI and fraud prevention in SACCOs, identifying strong links between AI implementation, system complexity, and employee training but lacking empirical data. Musa and Njeru (2023) examined AI's impact on SACCO operational performance and found a significant improvement but did not focus on fraud prevention. Mwirichia (2023) and Mugo (2022) found AI positively influenced operational and fraud detection performance in microfinance and SACCO contexts, respectively.

2.3. Data Analysis

The study utilized SPSS version 27 for data analysis. Descriptive statistics summarized the characteristics of key variables, including measures of central tendency and dispersion. Correlation analysis assessed the strength and direction of relationships between AI, fraud detection, regulatory compliance, and member engagement. Multiple regression analysis estimated the effect of AI on fraud detection and prevention while controlling other influencing variables. The regression model allowed quantification of how variations in AI implementation, system complexity, and training predict changes in fraud detection efficiency

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \varepsilon$$

Where: Y = Fraud detection and prevention

β_0 = y intercept of the regression equation; $\beta_1, \beta_2, \beta_3, \beta_4$ = are the regression coefficients

X_1 = AI implementation level

X_2 = AI system complexity

X_3 = Employee training on AI systems

X_4 = Regulatory compliance

ε = error term

3. RESULTS

3.1 AI Implementation Level

Table 1 results provide an overview of the descriptive statistics for AI implementation levels among the study SACCOs. The highest mean score of 4.64, with a standard deviation of 0.48, indicates that respondents strongly agree that their SACCO prioritizes AI implementation to enhance operational efficiency, with minimal variation in responses. Similarly, the statement assessing the effectiveness of current AI systems received a high mean score of 4.09 and a low standard deviation of 0.60, affirming the role of these systems in achieving organizational goals. Continuous investment in upgrading AI systems was rated positively, with a mean score of 4.05 and a standard deviation of 0.77, affirming the importance of updating AI systems. With a mean score of 4.06 and a standard deviation of 0.79, the use of AI was supported in fraud detection and risk mitigation. at a mean of 3.98 with a standard deviation of 0.73, encouragement in the use of AI tools showed moderate to high support for involvement in leveraging AI technologies.

Table 1: Descriptive Statistics for AI Implementation Level

Statements	N	Mean	Std. Dev
Our SACCO has fully integrated AI systems into its operations.	110	3.91	0.95
How would you rate the effectiveness of the current AI systems in achieving your organization's goals?	110	4.09	0.60
We continuously invest in upgrading our AI systems.	110	4.05	0.77
Our SACCO prioritizes AI implementation to enhance operational efficiency.	110	4.64	0.48
The management supports the extensive use of AI in fraud detection.	110	4.06	0.79
Employees are encouraged to use AI tools in their daily tasks.	110	3.98	0.73
Overall mean Score	110	4.12	0.76

The integration of AI systems into SACCO operations scored a mean of 3.91 with a standard deviation of 0.95, showing more variability, suggesting differing levels of integration across SACCOs. The overall mean score of 4.12 and a standard deviation of 0.76 demonstrate a strong,

consistent agreement across all statements, underscoring the significant role AI implementation plays in enhancing operational and fraud management capabilities within these institutions.

3.2 AI System Complexity

The results in Table 2 summarize the descriptive statistics for AI system complexity in deposit-taking SACCOs. The highest mean scores, at 4.09, with standard deviations of 0.67 and 0.73, respectively, affirm that the AI systems used in the SACCOs are highly complex and that dedicated teams are required to manage these systems and highlight the perceived sophistication of AI technologies within these organizations, necessitating specialized management.

Table 2: Descriptive Statistics for AI System Complexity

Statements	N	Mean	Std. Dev
The AI systems used in our SACCO are highly complex.	110	4.09	0.67
Understanding the functionalities of our AI systems requires specialized training.	110	3.95	0.71
Our AI systems are sophisticated but user-friendly.	110	3.68	1.14
The complexity of AI systems in our SACCO poses challenges for seamless operation.	110	3.64	0.88
We have a dedicated team to manage and oversee the AI systems due to their complexity.	110	4.09	0.73
The complexity of our AI systems necessitates regular updates and maintenance.	110	3.95	0.88
Overall Mean Score	110	3.90	0.60

The need for regular updates and maintenance due to system complexity and requirement for training to understand system functionalities had mean scores of 3.95 and standard deviations of 0.88 and 0.71, respectively, results suggesting a general acknowledgment of the ongoing efforts to effectively manage AI systems in SACCO operations.

Scoring a mean of 3.68 with a standard deviation of 1.14, the statement that ‘AI systems are sophisticated yet user-friendly’ had mixed perceptions about the ease of use of these systems despite their sophistication. The complexity of AI systems posing operational challenges received a lower mean of 3.64 with a standard deviation of 0.88, reflecting moderate agreement and variation in the experiences of respondents.

The overall mean score of 3.90 with a standard deviation of 0.60 underscores the recognition of AI system complexity across SACCOs; with moderate variability in perceptions and that efforts are being made to ensure their usability and integration into organizational processes

3.3 Employee Training on AI Systems

The results in Table 3 provide descriptive statistics on training regarding AI systems in deposit-taking SACCOs. The highest mean score of 4.16, with a standard deviation of 0.56, affirms that the quality of training on AI systems directly impacts fraud detection capabilities; it highlights the critical role of effective training in enhancing the operational efficiency of AI in fraud prevention. Workshops and seminars to enhance skills in AI systems were rated positively, with a mean score of 3.98 and a standard deviation of 0.63, reflecting consistent efforts by SACCOs to improve staff competency. Similarly, continuous training programs to update employees on AI advancements had a mean score of 3.95 and a low standard deviation of 0.56, affirming the importance of ongoing education in this rapidly evolving field.

Table 3: Descriptive Statistics for Employee Training on AI Systems

Statements	N	Mean	Std. Dev
All relevant employees have received comprehensive training on our AI systems.	110	3.73	0.62
The training provided on AI systems is sufficient for employees to perform their duties effectively.	110	3.86	0.55
Continuous training programs are in place to keep employees updated on AI advancements.	110	3.95	0.56
Employees feel confident using AI systems after receiving training.	110	3.82	0.72

The quality of training on AI systems directly impacts our fraud detection capabilities.	110	4.16	0.56
Regular workshops and seminars are conducted to enhance employees' skills in using AI systems.	110	3.98	0.63
Overall Mean Score	110	3.92	0.50

The adequacy of training for employees to perform duties effectively and their confidence in using AI systems after training scored means of 3.86 and 3.82 with a standard deviation of 0.55, while and 0.72 respectively, indicating the general satisfaction with the training provided with space for building greater employee confidence.

Comprehensive training for all relevant employees received a mean score of 3.73 and a standard deviation of 0.62, indicating moderate agreement and some variation in the extent of training coverage. The overall mean score of 3.92, with a standard deviation of 0.50, demonstrates a strong emphasis on employee training across SACCOs, to maximize the benefits of AI system implementation.

3.4 Regulatory Compliance

The results in Table 4 summarize the descriptive statistics for regulatory compliance concerning AI systems in deposit-taking SACCOs. The highest mean score of 4.41, with a standard deviation of 0.49, affirms that SACCOs regularly review and update their AI systems to ensure regulatory compliance, and emphasising aligning technological systems with regulatory frameworks.

Regulatory compliance in AI system implementation scored a mean of 4.05 and a standard deviation of 0.56, highlighting its importance in decision-making processes. With a mean of 4.01 and standard deviation of 0.55, compliance with regulations enhancing the effectiveness of AI fraud detection systems affirmed the perception of the role of regulatory adherence.

The influence of the regulatory environment on AI implementation strategies scored a mean of 3.92 with a standard deviation of 0.63, showing general agreement that regulations guide and shape AI adoption. The absence of regulatory issues related to AI systems had a mean score of 3.64 and

a standard deviation of 0.77, suggesting that while most SACCOs comply with regulations, some face occasional challenges.

Compliance with all relevant regulatory requirements scored the lowest mean of 3.36, with a standard deviation of 0.88, suggesting more variability in perceptions, reflecting differences in the extent of regulatory adherence among SACCOs. The overall mean score of 3.89, with a standard deviation of 0.47, demonstrates a strong commitment to regulatory compliance for effective and sustainable implementation of AI systems.

Table 4: Descriptive Statistics for Regulatory Compliance

Statements	N	Mean	Std. Dev
Our SACCO's AI systems comply with all relevant regulatory requirements.	110	3.36	0.88
Regulatory compliance is a key consideration in the implementation of AI systems.	110	4.05	0.56
We have not faced any regulatory issues related to our AI systems.	110	3.64	0.77
Our SACCO regularly reviews and updates its AI systems to ensure regulatory compliance.	110	4.41	0.49
Compliance with regulations enhances the effectiveness of our AI fraud detection systems.	110	4.01	0.55
The regulatory environment positively influences our AI implementation strategies.	110	3.92	0.63
Overall Mean Score	110	3.89	0.47

3.5 Regression Analysis

The regression results in Table 5 show the model summary, highlighting the strength and explanatory power of the predictors in fraud detection and prevention. The R value of 0.964 indicates a strong positive relationship between the predictors and the dependent variable. The R Square value of 0.928 shows 92.8% of the variance in fraud detection and prevention can be

explained by these predictors, while the Adjusted R Square of 0.926 confirms the model's robustness when adjusted for the number of predictors.

Table 5: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.964 ^a	.928	.926	.228918

a. Predictors: (Constant), Regulatory compliance, AI implementation level, AI system complexity, Employee training on AI systems

3.6 ANOVA

Table 6 presents the ANOVA results, assessing the overall significance of the regression model. The F-statistic of 340.679 and the associated p-value of 0.000 indicate that the model is statistically significant at the 5% level. This confirms that the combination of AI implementation level, AI system complexity, employee training on AI systems, and regulatory compliance significantly predicts fraud detection and prevention. The low residual sum of squares (5.502) compared to the regression sum of squares (71.411) further supports the model's strong explanatory power.

Table 6: ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	71.411	4	17.853	340.679	.000 ^b
	Residual	5.502	105	.052		
	Total	76.913	109			

a. Dependent Variable: Fraud detection and prevention

b. Predictors: (Constant), Regulatory compliance, AI implementation level, AI system complexity, Employee training on AI systems

Table below details the coefficients of the regression model, showing the individual contributions of each predictor to fraud detection and prevention. Regulatory compliance has the highest standardized beta coefficient (0.739), indicating it is the most significant predictor, with a t-value

of 10.683 and a p-value of 0.000. This underscores its critical role in enhancing fraud prevention measures. AI implementation level has a standardized beta of 0.349, with a t-value of 5.846 and a p-value of 0.000, highlighting its substantial positive influence on fraud detection.

AI system complexity has a standardized beta coefficient of 0.308, a t-value of 4.542, and a p-value of 0.000, indicating that system sophistication significantly enhances fraud detection and prevention capabilities. Employee training on AI systems, with a standardized beta of 0.227, a t-value of 3.325, and a p-value of 0.001, also makes a positive and statistically significant contribution, emphasizing the importance of equipping staff with the skills to effectively utilize AI tools. Together, these results demonstrate that all predictors significantly influence fraud detection and prevention, with regulatory compliance having the strongest impact.

Table 7: Coefficients

		Unstandardized		Standardized		
		Coefficients		Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	(Constant)	1.131	.193		5.863	.000
	AI implementation level	.418	.072	.349	5.846	.000
	AI system complexity	.231	.051	.308	4.542	.000
	Employee training on AI systems	.218	.066	.227	3.325	.001
	Regulatory compliance	.708	.066	.739	10.683	.000

a. Dependent Variable: Fraud detection and prevention

4. DISCUSSION

Findings of this study align with the guiding theories, Technology Acceptance Model and Fraud Triangle Theory and complement the empirical evidence from previous studies. According to TAM, the perceived usefulness and ease of use of AI technologies influence their adoption. This

study confirmed that AI implementation level significantly improves fraud detection and prevention ($\beta = 0.349$, $p = 0.000$), echoing the findings of Kotagiri (2023), establishing a similar positive relationship in the U.S. banking sector. The study also supports the Diffusion of Innovations Theory that complexity and relative advantage are critical factors in technology adoption. AI system complexity ($\beta = 0.308$, $p = 0.000$) was found to have a significant influence, resonating with Mohanty and Mishra (2023) and Martínez et al. (2022), emphasizing the role of system sophistication in fraud prevention.

The Fraud Triangle Theory underscores the importance of addressing opportunities for fraud through robust systems and employee oversight. This study identified training on AI systems ($\beta = 0.227$, $p = 0.001$) as significant in fraud detection, supporting the findings of Mohanty and Mishra (2023), highlighting the criticality of competency in leveraging AI technologies. Regulatory compliance emerged the strongest predictor ($\beta = 0.739$, $p = 0.000$), aligning with the study's conceptual framework filling a gap noted in studies by Martínez et al. (2022) and Găbudeanu et al. (2021), neither of which addressed compliance. This finding underscores the role of adherence to legal and operational standards in enhancing fraud prevention mechanisms.

The study's results mirror global trends while addressing contextual differences in Kenya. Unlike Zhu et al. (2021), who focused on real-time analytics and machine learning in Chinese banking context, it emphasized regulatory compliance, crucial in a developing economy. Locally, Mwavali (2024) and Mugo (2022) confirmed that AI implementation and system complexity positively influence fraud detection and prevention in Kenyan commercial banks and SACCOs. However, this study incorporates regulatory compliance as a critical variable, addressing the conceptual gap in their studies.

The findings reflect differences in methodology and focus compared to previous studies. While Millan and Ibua (2023) provided a theoretical foundation for the role of AI in fraud prevention in Kenyan SACCOs, this study empirically tested these theories, addressing the methodological gap. Additionally, the findings complement Musa and Njeru (2023) and Mwirichia (2023), who explored the broader impact of AI on operational performance rather than fraud detection. By

focusing specifically on fraud prevention, this study provides deeper insights into how AI implementation and related factors directly combat fraudulent activities in SACCOs.

5. CONCLUSION AND RECOMMENDATIONS

Fraud detection and prevention involve strategies and technologies that identify and mitigate fraudulent activities. Detection focuses on recognizing anomalies within transactions (Razaque et al., 2022), while prevention includes implementing policies and controls to deter fraud (Odeyemi et al., 2024). Key performance measures include fraud detection rate, response time to fraudulent incidents (Mandal, 2023), and reduction in financial losses (Ameyaw et al., 2024). Collectively, these measures assess the effectiveness of organizational strategies against fraudulent activities.

5.1 Recommendations

A supportive framework for the adoption of artificial intelligence is supposed to be in place to enhance fraud detection and prevention in deposit-taking SACCOs. This includes updating regulatory guidelines to accommodate emerging AI technologies and aligning with global best practices. Such policies should incentivize SACCOs to invest in AI systems by offering tax breaks or grants for technological upgrades, particularly for smaller institutions facing financial constraints.

SACCOs should prioritize the full integration of AI systems into their operations. Management teams are encouraged to allocate sufficient resources for advanced AI technologies, focusing on areas such as real-time fraud monitoring, predictive analytics, and automated fraud detection tools accompanied by robust strategic planning to ensure that AI solutions are tailored to the unique operational needs and risk profiles of each SACCO.

Continuous employee training is essential to maximize the effectiveness of AI systems in fraud prevention. Investment in regular training and workshops to keep employees updated on advancements in AI technologies and fraud management practices is a necessity. Collaboration with training institutions or AI solution providers help to develop customized training modules that address specific skill gaps. Fostering a culture of innovation and employee engagement will encourage staff to embrace AI tools and leverage them effectively.

Regulatory compliance must be prioritized for SACCOs to enhance the effectiveness of AI-driven fraud management systems. SACCOs are advised to establish internal audit teams to monitor compliance with regulatory standards and conducting periodic reviews of AI systems. This will ensure that fraud detection mechanisms are aligned with legal requirements and operational best practices. The introduction of industry-wide benchmarking standards by regulators can help SACCOs assess their progress and adopt best practices from leading institutions.

REFERENCES

- Aburbeian, A. M., Owda, A. Y., & Owda, M. (2022). A technology acceptance model survey of the metaverse prospects. *Ai*, 3(2), 285-302.
- Acikgoz, F., Elwalda, A., & De Oliveira, M. J. (2023). Curiosity on cutting-edge technology via theory of planned behavior and diffusion of innovation theory. *International Journal of Information Management Data Insights*, 3(1), 100-152.
- Adelakun, B. O., Onwubuariri, E. R., Adeniran, G. A., & Ntiakoh, A. (2024). Enhancing fraud detection in accounting through AI: Techniques and case studies. *Finance & Accounting Research Journal*, 6(6), 978-999.
- Ahmed, S. F., Alam, M. S. B., Hassan, M., Rozbu, M. R., Ishtiaq, T., Rafa, N., ...& Gandomi, A. H. (2023). Deep learning modelling techniques: current progress, applications, advantages, and challenges. *Artificial Intelligence Review*, 56(11), 13521-13617.
- Alfadda, H. A., & Mahdi, H. S. (2021). Measuring students' use of zoom application in language course based on the technology acceptance model (TAM). *Journal of Psycholinguistic Research*, 50(4), 883-900.
- Alowais, S. A., Alghamdi, S. S., Alsuhebany, N., Alqahtani, T., Alshaya, A. I., Almohareb, S. N., ...& Albekairy, A. M. (2023). Revolutionizing healthcare: the role of artificial intelligence in clinical practice. *BMC medical education*, 23(1), 672-689.
- Ameyaw, M. N., Idemudia, C., & Iyelolu, T. V. (2024). Financial compliance as a pillar of corporate integrity: A thorough analysis of fraud prevention. *Finance & Accounting Research Journal*, 6(7), 1157-1177.
- Aripin, R. M., Mahmud, R., Sabli, N., & Tapsir, R. (2022). Fraudulent Financial Reporting in Malaysia: From Fraud Triangle Theory Perspective. *Advanced International Journal of Banking, Accounting and Finance*, 4(11), 30-48.

- Bansal, U., Bharatwal, S., Bagiyam, D. S., &Kismawadi, E. R. (2024). Fraud Detection in the Era of AI: Harnessing Technology for a Safer Digital Economy. In *AI-Driven Decentralized Finance and the Future of Finance* (pp. 139-160). IGI Global.
- Batchu, R. K. (2023). Artificial Intelligence in Credit Risk Assessment: Enhancing Accuracy and Efficiency. *International Transactions in Artificial Intelligence*, 7(7), 1-24.
- Bao, Y., Hilary, G., &Ke, B. (2022).Artificial intelligence and fraud detection. *Innovative Technology at the Interface of Finance and Operations*.1(7);223-247.
- 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.
- Bokolo, A. J. (2023). Examining the adoption of sustainable eMobility-sharing in smart communities: diffusion of innovation theory perspective. *Smart Cities*, 6(4), 2057-2080.
- Cempakasari, I., Kuntadi, C., &Rosdiana, D. (2023). Factors affecting fraud detection and prevention: internal control, whistleblowing system and moral. *Dinasti International Journal of Digital Business Management*, 4(3), 508-516.
- Chukwuma, P. (2023). Integrating diffusion of innovations and theory of planned behavior to predict intention to adopt electric vehicles in Rwanda. *European Journal of Business and Strategic Management*, 8(1), 1-15.
- Clark, T., Foster, L., Bryman, A., & Sloan, L. (2021). *Bryman's social research methods*.Oxford university press.
- Cooper, D. R., & Schindler, P. S. (2018). *Business research methods*. New Delhi: Tata McGraw-Hill Publishing Company Limited
- Cressey, D. R. (1953). Other people's money; a study of the social psychology of embezzlement.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 8(3);319-340.
- Dhameliya, N. (2023). Revolutionizing PLC Systems with AI: A New Era of Industrial Automation. *American Digits: Journal of Computing and Digital Technologies*, 1(1), 33-48.
- Donald, C,(1953). The fraud triangle. *Security Journal*, 29, 107-121.

- Fundi, N. E., &Wamugo, L. (2023). Effect of deposit risk on financial performance of deposit taking sacco in Nairobi City County, Kenya. *International Academic Journal of Economics and Finance*, 3(9), 453-462.
- Fussell, S. G., & Truong, D. (2022). Using virtual reality for dynamic learning: an extended technology acceptance model. *Virtual Reality*, 26(1), 249-267.
- Găbudeanu, L., Brici, I., Mare, C., Mihai, I. C., &Șcheau, M. C. (2021). Privacy intrusiveness in financial-banking fraud detection. *Risks*, 9(6), 104-113.
- Gichuhi, D. (2021). *Effect of Financial Risk on Efficiency of Deposit Taking Savings and Credit Cooperatives in Nairobi County, Kenya* (Doctoral dissertation, University of Nairobi).
- 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.
- Hassan, M., Aziz, L. A. R., &Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, 6(1), 110-132.
- Herbenita, H., Rahmawati, A., &Surwanti, A. (2022). Potential of Fraud Financial Statements: The Fraud Triangle. *Central Asian Journal of Innovations on Tourism Management and Finance*, 3(10), 201-212.
- Hsu, C. L., & Lin, J. C. C. (2023). Understanding the user satisfaction and loyalty of customer service chatbots. *Journal of Retailing and Consumer Services*, 7(1), 203-211.
- Huong, P. T., &Duc, N. L. (2023). The perceptions of prospective digital transformation adopters: An extended diffusion of innovations theory. *TEM Journal*, 12(1);33-42.
- Ismail, R. B. (2024). A Comprehensive study on the application of convolutional neural networks in fraud detection and prevention in modern banking. *Advances in Intelligent Information Systems*, 9(4), 11-20.
- Issa, H., Jabbouri, R., & Palmer, M. (2022). An artificial intelligence (AI)-readiness and adoption framework for AgriTech firms. *Technological Forecasting and Social Change*, 18(2), 821-874.
- Kagias, P., Cheliatsidou, A., Garefalakis, A., Azibi, J., &Sariannidis, N. (2022). The fraud triangle—an alternative approach. *Journal of Financial Crime*, 29(3), 908-924.

- Karmila, Y., &Wahad, A. (2024). Determinants of fraud detection and prevention PT Perkebunan Nusantara XIV Takalar. *Formosa Journal of Applied Sciences*, 3(2), 759-774.
- Kelly, S., Kaye, S. A., & Oviedo-Trespalacios, O. (2023). What factors contribute to the acceptance of artificial intelligence? A systematic review. *Telematics and Informatics*, 7(7), 901-925.
- Kok, S. L., &Siripipatthanakul, S. (2023). Artificial Intelligence (AI) Adoption: The Case of the Malaysian Financial Industry. *Advance Knowledge for Executives*, 2(4), 1-15.
- 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.
- Mahya, L., Tarjo, T., Sanusi, Z. M., &Kurniawan, F. A. (2023). Intelligent Automation of fraud detection and investigation: A Bibliometric Analysis Approach. *JurnalReviuAkuntansidanKeuangan*, 13(3), 588-613.
- Mandal, A. (2023). Fathoming fraud: unveiling theories, investigating pathways and combating fraud. *Journal of Financial Crime*, 3(9);21-29.
- Martínez, B., Allmendinger, R., Khorshidi, H. A., Papamarkou, T., Feitas, A., Trippas, J., ...& Benson, K. (2023). Mapping the State of the Art: Artificial Intelligence for Decision Making in Financial Crime. *Cybersecurity for Decision Makers*, 3(7);199-213.
- Millan, E. N., &Ibua, M. (2023). Effect of Process Digitalization on Loan Performance of Deposit Taking SACCOs in Mombasa County.
- Mohanty, B., & Mishra, S. (2023). Role of Artificial Intelligence in Financial Fraud Detection. *Academy of Marketing Studies Journal*, 27(S4);32-41.
- Muhsyaf, S. A., &Pituringasih, E. (2024). Determinants of fraud detection and prevention with monitoring center for prevention (MCP) as moderation. *International Journal of Multicultural and Multireligious Understanding*, 11(2), 380-396.
- Mugo, D. M. (2022). Transforming savings and credit cooperatives societies in Kenya using AI and mobile technology services. *International Journal of Business Information Systems*, 40(4), 560-579.
- Musa, S. K., &Njeru, A. W. (2023). Effect of Digital Financial Innovation on the Financial Performance of SACCOs in Nairobi City Centre, Kenya. *International Journal of Social Science and Humanities Research*, 1(1);32-39.

- Mwavali, A. (2024). Framework for Mitigating Phishing E-mail in the Kenyan Banking Industry Using Artificial Intelligence (AI). *International Journal of Technology and Systems*, 9(2), 40-66.
- Mwirichia, C. M. (2023). *Effect of Process Innovations on Financial Performance of Microfinance Institutions in Nairobi County, Kenya* (Doctoral dissertation, KeMU).
- Mytnyk, B., Tkachyk, O., Shakhovska, N., Fedushko, S., & Syerov, Y. (2023). Application of artificial intelligence for fraudulent banking operations recognition. *Big Data and Cognitive Computing*, 7(2), 81-93.
- Nazareno, L., & Schiff, D. S. (2021). The impact of automation and artificial intelligence on worker well-being. *Technology in Society*, 6(7), 651-679.
- Nguyen, T. L., Nguyen, V. P., & Dang, T. V. D. (2022). Critical factors affecting the adoption of artificial intelligence: An empirical study in Vietnam. *The Journal of Asian Finance, Economics and Business*, 9(5), 225-237.
- Nguyen, C. T., & Van Nguyen, B. (2023). Ethical Issues of Vietnamese Auditors: Applying the Fraud Triangle Model. *International Journal of Professional Business Review*, 8(6), e02599-e02599.
- Noreen, U., Shafique, A., Ahmed, Z., & Ashfaq, M. (2023). Banking 4.0: Artificial intelligence (AI) in banking industry & consumer's perspective. *Sustainability*, 15(4), 36-82.
- Ngeno, J., Naibei, I. K., & Langat, P. (2023). Does Corporate Governance affect Earnings Management? A case study of Deposit Taking Saccos in South Rift Region, Kenya.
- Odeyemi, O., Mhlongo, N. Z., Nwankwo, E. E., & Soyombo, O. T. (2024). Reviewing the role of AI in fraud detection and prevention in financial services. *International Journal of Science and Research Archive*, 11(1), 2101-2110.
- Odhiambo, O. (2022). *Exploring the Machine Learning and Artificial Intelligence Algorithm Needed to Detect Healthcare Financial Statement Anomalies* (Doctoral dissertation, Colorado Technical University).
- Onjura, C. O., Muia, M. F. M., & Aseka, E. (2021). Influence of information capital readiness on implementation of customer asset management by saccos licensed to undertake deposit-taking in Kenya. *International Journal of Business Management and Economic Review*, 4(5);23-29.

- Opati, T. Z. (2022). Ethical new product development: A case of digital loans products in Kenya. In *Products for Conscious Consumers: Developing, Marketing and Selling Ethical Products* (pp. 185-204). Emerald Publishing Limited.
- Park, I., Kim, D., Moon, J., Kim, S., Kang, Y., &Bae, S. (2022). Searching for new technology acceptance model under social context: analyzing the determinants of acceptance of intelligent information technology in digital transformation and implications for the requisites of digital sustainability. *Sustainability*, 14(1), 579-583.
- Priya, G. J., &Saradha, S. (2021). Fraud detection and prevention using machine learning algorithms: a review. In *2021 7th International Conference on Electrical Energy Systems (ICEES)* (pp. 564-568).IEEE.
- Rahman, M. J., &Jie, X. (2024). Fraud detection using fraud triangle theory: evidence from China. *Journal of Financial Crime*, 31(1), 101-118.
- Rahmawati, L., &Pradata, B. G. (2023). The influence of corporate culture and internal control systems on the prevention of merchandise fraud. *JurnalIlmiahManajemenKesatuan*, 11(3), 1483-1494.
- Razaque, A., Frej, M. B. H., Bektemyssova, G., Amsaad, F., Almiani, M., Alotaibi, A., ...&Alshammari, M. (2022). Credit card-not-present fraud detection and prevention using big data analytics algorithms. *Applied Sciences*, 13(1), 57-68.
- Rogers, E. M. (1962). *Bibliography on the Diffusion of Innovations*.
- Rodrigues, V. F., Policarpo, L. M., da Silveira, D. E., da Rosa Righi, R., da Costa, C. A., Barbosa, J. L. V., ... &Arcot, T. (2022). Fraud detection and prevention in e-commerce: A systematic literature review. *Electronic Commerce Research and Applications*, 56, 101207.
- Romero-Carazas, R., Espíritu-Martínez, A. P., Aguilar-Cuevas, M. M., Usuriaga-Palacios, M. N., Aguilar-Cuevas, L. A., Espinoza-Véliz, M. Z., ... & Gutiérrez-Monzón, S. G. (2024). Forensic auditing and the use of artificial intelligence: A bibliometric analysis and systematic review in Scopus between 2000 and 2024. *Heritage and Sustainable Development*, 6(2), 415-428.
- Salawu, M. K., Oyewobi, I. A., &Adejumo, O. A. (2023). Internal control system, risk management practice and fraud detection and prevention among selected state governments in southwestern Nigeria. *TWIST*, 18(4), 123-134.

- Sambrow, V. D. P., & Iqbal, K. (2022). Integrating Artificial Intelligence in Banking Fraud Prevention: A Focus on Deep Learning and Data Analytics. *Eigenpub Review of Science and Technology*, 6(1), 17-33.
- Shahzadi, K., Alim, W., & Khan, S. N. (2024). Do the fraud triangle components fuel complex financial fraud? A study of nonfinancial firms in Pakistan. *Journal of Financial Crime*, 3(7);32-41.
- 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.
- Shihembetsa, E. (2021). *Use of artificial intelligence algorithms to enhance fraud detection in the Banking Industry* (Doctoral dissertation, University of Nairobi).
- Siagian, A. O., Manurung, A. H., Widyastuti, T., & Rony, Z. T. (2023). Analysis of internal control, good corporate governance and reporting system against fraud. *International Journal of Management Research and Economics*, 1(4), 150-166.
- Wekesa, J. M. (2023). *Effect of Financial Technology on Financial Performance of Deposit-taking Savings and Credit Cooperative Societies in Nairobi County, Kenya* (Doctoral dissertation, University of Nairobi).
- Wuryandini, A. R., Pakaya, L., & Husain, S. P. (2023). Fraud Control to Strengthen Internal Control Systems in Local Government. *International Journal of Applied Business and International Management (IJABIM)*, 8(2), 85-98.
- Yang, L., BashiruDanwana, S., & Yassanah, I. F. L. (2021). An empirical study of renewable energy technology acceptance in Ghana using an extended technology acceptance model. *Sustainability*, 13(19), 67-91.
- Yuhertiana, I., & Amin, A. H. (2024). Artificial Intelligence Driven Approaches for Financial Fraud Detection: A Systematic Literature Review. *KnE Social Sciences*, 2(8);448-468.
- Zakaria, S., Manaf, S. M. A., Amron, M. T., & Suffian, M. T. M. (2023). Has the world of finance changed? A review of the influence of artificial intelligence on financial management studies. *Information Management and Business Review*, 15(4), 420-432.
- Zayed, L. M. M., Nour, M. I., Al Attar, K., Almubaideen, H., & Abdelaziz, G. A. M. (2024). Role of Artificial Intelligence (AI) in Accounting Information Systems in Detecting Fraud.

In Artificial Intelligence and Economic Sustainability in the Era of Industrial Revolution 5.0 (pp. 397-409). Cham: Springer Nature Switzerland.

- Ziorklui, J. E. K., Ampofo, F. O., Nyonyoh, N., &Antwi, B. O. (2024). Effectiveness of internal controls mechanisms in preventing and detecting fraud. *Finance & Accounting Research Journal*, 6(7), 1259-1274.
- Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., & Li, J. (2021). Intelligent financial fraud detection practices in the post-pandemic era. *The Innovation*, 2(4);65-73.
- Zoubi, M., ALfaris, Y., Fraihat, B., Otoum, A., Nawasreh, M., &ALfandi, A. (2023). An extension of the diffusion of innovation theory for business intelligence adoption: A maturity perspective on project management. *Uncertain Supply Chain Management*, 11(2), 465-472.