ACADEMIA International Journal for Social Sciences
Volume 5, Issue 1, 2026 ISSN-L (Online): 3006-6638

Impact of Artificial Intelligence on Fraud Detection in Retail Banking: A Quantitative Study

Javeed Iqbal
javedamjadmarwat@gmail.com
PhD Scholar, Department of Public Administration, Gomal University, Dera Ismail Khan, KP, Pakistan

Zia Ullah Khan
ziakhankust@gmail.com
PhD Scholar, Kohat University of Science and Technology Kohat, Pakistan

Ishtiaq Ahmad Bajwa
ishiforce@gmail.com
Assistant Professor, Al Yamamah University, Kingdom of Saudi Arabia (KSA)

Muhammad Shehzad Dhedhi
shehzaddhedhi@gmail.com
Founder CFO Club

Ubaid Ullah
ubaid66221@gmail.com
Visiting Lecturer Business Education Department, IER. University of the Punjab Lahore, Pakistan

Safdar Marwat
safdariqbal0700@gmail.com

Corresponding Author: * Javeed Iqbal javedamjadmarwat@gmail.com

Received: 03-12-2025 **Revised:** 17-12-2025 **Accepted:** 01-01-2026 **Published:** 15-01-2026

ABSTRACT

Background: *Fraud in retail banking has taken a dynamic and technologically-oriented threat environment. Conventional rule-based fraud detection solutions are no longer adequate in detecting the new fraud schemes and sealing the operational loopholes. The AI-based fraud detection systems provide adaptive anomaly detection, behavioral modeling, and risk scoring in real-time. Nevertheless, predictive capability will not be effective alone in such systems, but also in the quality of system design and organizational enablement in frontline banking operations.* ***Purpose:*** *This paper will analyze the role of AI System Design Quality and AI Organizational Enablement in the effectiveness of Fraud Control in retail banking. It also explores how Perceived Loophole Detection Capability (PLDC) plays a mediating role in the transfer of AI system attributes to better fraud containment results.* ***Methods:*** *The quantitative cross-sectional survey design was used among the retail banking operations and call-center employees, who dealt with fraud alerts. Analysis of data was performed with the help of Partial Least Squares Structural Equation Modeling (PLS-SEM) according to the recommended methodology (Hair et al., 2022). Constructs were conceptualized into reflective-reflective higher-order elements.* ***Results:*** *The results show that AI System Design Quality and Organizational Enablement have a positive and significant impact on PLDC that consequently improves Fraud Control Effectiveness. The mediation analysis proves that the relationship between AI system factors and the results of the fraud control is mediated by PLDC partially.* ***Conclusion:*** *AI is not only used to increase technical accuracy but also perceived ability to detect operational blind spots, which are used to mitigate fraud. To maximize the performance of fraud control, it is important to have effective system design and organizational support.*

Keywords: *Artificial Intelligence; Fraud Detection; Retail Banking; PLS-SEM; Operational Risk; Explainable AI*

INTRODUCTION

Prevention of fraud is one of the major operational issues in the retail banking. As financial services have progressively become digitized, fraudulent activities have taken a more dynamic and complex form that can no longer be easily identified by using fixed set rule-based surveillance. Conventional methods of fraud detection are based on the preset thresholds and manually designed rules, which are not capable of detecting new behavioral patterns and fraud schemes (Bolton and Hand, 2002; Bhattacharyya et al., 2011). These fixed systems leave operational blind spots, weaknesses in the processes or gaps in the monitoring systems that cannot be identified until they result in losses as the underlying fraudsters keep evolving.

Fraud detection systems using artificial intelligence (AI) have become one of the strategic solutions to these restrictions. Machine learning models could be used to analyze a high amount of transactional data, detect abnormal patterns, and dynamically adjust risk scores in real-time (Carcillo et al., 2018; Ali et al., 2022). More current trends involve explainable AI methods that can give interpretable results thus improving user comprehension and decision support (Zhou, 2023). The effectiveness of AI systems to the organization largely relies on their characteristics, despite the level of technology.

Retail banking Fraud detection is not entirely computerized. It entails the interplay between humans and AI in which frontline employees go through alerts, validate transactions, and interact with customers and escalate cases. Therefore, the performance of the AI systems should be studied not only in terms of predictive accuracy but also in terms of the organizational management. According to the Information Systems (IS) Success Model, the quality of the systems and information quality affect the perceptions and net benefits of the users (DeLone and McLean, 2003; Petter et al., 2008). Likewise, research on the adoption of technologies shows that system usability and organizational support play an important role in influencing the resultant usage (Davis, 1989; Venkatesh et al., 2003).

Nevertheless, little work has been done to explore how the nature of AI systems and organizational enablement can complement each other to improve fraud containment by better detecting monitoring blind spots. The proposed research presents the construct of Perceived Loophole Detection Capability (PLDC) to identify perceptions of the employees that AI systems decrease monitoring gaps, identify new fraud schemes, and detect anomalies that were not detected by conventional rule-based systems.

The research has three contributions to the literature. First, it applies AI adoption researches to the coverage of operational risk management by connecting the quality of the system design and organizational enabling to the result of fraud control. Second, it theorizes that PLDC is a mediating process which clarifies how AI capabilities are converted into the effectiveness of fraud containment. Third, it uses a PLS-SEM model, which aligns with recent organizational survey studies in the banking setting (Hair et al., 2022; Iqbal et al., 2025).

This study is carried out in the following research question:

What is the Relationship between the AI System Design Quality and AI Organizational Enablement and Fraud Control Effectiveness and whether Perceived Loophole Detection Capability mediates?

LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

AI-Based Fraud Detection in Retail Banking

Retail banking fraud detection has developed to be beyond basic manual assessments and monitored rules to dynamically functioning artificial intelligence (AI) systems that can sense abnormalities in real-time. The traditional fraud detection methods are based on the preset cutoffs and human-made rules, which Fastly become obsolete along with the fraud methods (Bolton and Hand, 2002; Bhattacharyya et al., 2011). These systems are not able to generalize outside patterns of known fraud, and accordingly have operational blind spots when fraudsters change their behavioral tactics or when they take advantage of inflexible monitoring logic.

The anomaly detection, behavioral profiling, and supervised learning AI-based systems are capable of processing large amounts of transactional data to detect subtle and emerging irregularities (Carcillo et al., 2018). Empirical studies indicate that machine learning systems are more effective than traditional rule-based systems in recall and adaptability, particularly in dynamic environments (Ali et al., 2022). Moreover, explainable AI can be seen as a solution to the problem of interpretability since it helps provide clear explanations of the flagged transactions, thus, decreasing the level of algorithmic opacities and increasing the comprehension offered to the user (Zhou, 2023).

Nevertheless, predictive performance is not a factor that defines the overall performance of fraud detection. The frontline employees of Banking in Retail deal face-to-face with AI-generated notifications. They understand risk scores, approve of suspicious transactions, interact with customers, and ramp up cases as needed. Thus, the organizational influence of AI is not solely based on the accuracy of algorithms, but on system design and organizational environment. Information systems-wise, it is the perception of users and the conditions in organizations, that mediate performance impacts of technology and not a technical attribute only driven performance (DeLone and McLean, 2003; Petter et al., 2008).

Theoretical Foundations

The research is based on four theoretical perspectives that complement each other to explain the effects of AI systems into operational results in a fraud detection environment.

First, the Information Systems (IS) Success Model is based on the assumption that the quality of the system can affect the performance of the organization mainly via the user rating and perceived net benefits (DeLone and McLean, 2003). Reliability, usability, and transparency are technical characteristics that determine how end-users view the value of the system and which further determines how performance of the organization.

Second, the sociotechnical theory maintains that, performance gains do not occur in isolation because of technology. Rather, they are the results of the interplay of the technical aspects and the human interpretations in the organizational processes. The AI alerts can bring value only to the extent that employees recognize, trust, and implement them properly in the decision-making.

Third, explainable AI literature points out that, transparency improves interpretability and trust in the user as opposed to driving benefits directly. When the employees know the reasons behind flagging a transaction, they will trust system outputs and use them as a productive tool to investigate a fraud.

Lastly, operational risk management structures posit that it is best to contain risks when personnel have the feeling that control systems are successful in their quest to recognize their weaknesses and arising threats.

Perceived detection capability is then considered as a significant psychological and operational mechanism that would interconnect systems characteristics with enhanced fraud mitigation.

On the whole, these views confirm the choice of Perceived Loophole Detection Capability (PLDC) as the main factor in which AI System Design Quality and AI Organizational Enablement determine the level of Fraud Control.

AI System Design Quality

The IS Success Model suggests that the quality of the system is one of the determinants of perceived benefits and organizational.

performance (DeLone and McLean, 2003). Reliability, responsiveness, usability, and compatibility with existing workflows are part of system quality (Petter et al., 2008). Transparency and explainability are now critical additions to system quality in AI contexts due to the fear of algorithmic opacity and accountability.

The ease of use is perceived to have an effect on cognitive effort and operational efficiency (Davis, 1989). The responsive and intuitive systems will also minimize cognitive burden and provide quicker responses to fraud notifications. Transparency empowers the trust of the users by explaining the construction of risk scores and flags of anomalies. The studies of organizational openness indicate that the availability of comprehensible information increases trust and effectiveness in decision-making (Schnackenberg and Tomlinson, 2014). Explainable outputs in AI-based fraud detection give the employees the opportunity to provide an excuse and effectively explain to customers about the suspicious transaction (Zhou, 2023).

In case AI systems can be trusted, be intuitive, and show transparency, the workers will feel that they are able to detect weak spots that are not recognized by the old rule-based systems. Such impressions lead to the assumption that AI bridging the monitoring gaps and improving the process of fraud containment.

In this respect, AI System Design Quality is defined as a conceptualized higher-order construct that entails system quality, ease of use and transparency.

H1: AI System Design Quality positively influences Perceived Loophole Detection Capability.

AI Organizational Enablement

Effective adoption of AI needs organizational alignment, managerial commitment and ability building. Facilitating conditions and management support have been found to be the major determinants of effective use of technology as indicated by technology adoption research (Venkatesh et al., 2003; Premkumar and Roberts, 1999). The literature on governance also focuses on structured decision rights and accountability mechanisms as facilitators of technology performance (Weill and Ross, 2004).

The introduction of AI into organizations can be facilitated by training, distributing resources, and outlining the procedures (Hradecky et al., 2022). In the absence of a well-organized enablement, employees can misinterpret the results of AI, overuse the capabilities of the systems, or go back to manual operations. A lack of training may expand the uncertainty of decisions making and decrease operational effectiveness in fraud monitoring settings that are time-sensitive.

A successful organizational enabling empowerment enhances the competency and confidence of the employees in interpreting AI-generated risk scores and anomaly warnings. This kind of support also creates

an impression that AI systems are effective in reducing the blind spots of monitoring as well as identifying the new fraud techniques.

AI Organizational Enablement is considered as reflective higher-order construct that is made of organizational support and training facilitation.

H2: AI Organizational Enablement positively influences Perceived Loophole Detection Capability.

Perceived Loophole Detection Capability

Weaknesses in monitoring logic, coordination processes, and response mechanisms are part of the weaknesses that are usually exploited by fraud schemes. These flaws are areas of weaknesses in operations that undermine the fight against fraud. Although previous studies have given priority to technical performance indicators, including accuracy, precision, and recall (Ali et al., 2022; Carcillo et al., 2018), these variables do not reflect the perception of employees in terms of the system to reveal hidden vulnerabilities.

In line with the IS Success model, the perceived net benefits intermediary the connection between the system attributes and organizational outcomes (DeLone and McLean, 2003; Rai et al., 2002). Drawing on this argument, Perceived Loophole Detection Capability (PLDC) indicates the beliefs of employees that AI-based systems will detect hidden frauds, detect new fraud trends, and discover monitor blind spots not yet detected by rule-based systems.

The employees will report more improvement in the process and the outcome of fraud monitoring when they believe that AI can spot such loopholes.

The effectiveness of fraud control involves the capability of the organization to prevent fraud matters.

H3: Perceived Loophole Detection Capability positively influences Fraud Control Effectiveness.

Fraud Control Effectiveness

The effectiveness of fraud control indicates the level of the quality of the fraud prevention and response systems. It incorporates less monetary losses, high rate of detection, low rate of false-positive, and quicker resolution of the case (Ngai et al., 2011). Operational risk frameworks focus on the strong control systems in order to reduce financial and reputational risks (Basel Committee, 2011).

Based on the premises of the IS Success Model and the operational risk logic, the system attributes are proposed to produce direct and indirect impacts on the performance outcomes based on the perceived benefits. Thus, the mediation of the effect of the AI System Design Quality and AI Organizational Enablement on the fraud control outcomes is investigated to find out whether the effects are mediated by the perceived detection ability of employees or not.

System design and organizational enablement may also have a direct performance impact, although theory points to the central role played by perceived capability.

H4a: Perceived Loophole Detection Capability mediates the relationship between AI System Design Quality and Fraud Control Effectiveness.

H4b: Perceived Loophole Detection Capability mediates the relationship between AI Organizational Enablement and Fraud Control Effectiveness.

Although theory suggests that perceived capability plays a central role, system design and organizational enablement may also exert direct performance effects.

H5: AI System Design Quality positively influences Fraud Control Effectiveness.

H6: AI Organizational Enablement positively influences Fraud Control Effectiveness.

METHODOLOGY

Research Design and Philosophy

The research philosophy used in this study is positivism, which is oriented towards objective measurements and testing hypotheses, which entails quantitative research methods. Positivism suits since the research focuses on the causation relationship of latent constructs, which is conducted with a systematic survey tool and statistical analysis. The study is cross-sectional and explanatory in nature and it is intended to establish the hypothesized relationships among AI System Design Quality, AI Organizational Enablement, Perceived Loophole Detection Capability (PLDC) and Fraud Control Effectiveness.

An approach was chosen to be quantitative so that the structural modeling could be conducted with the help of Partial Least Squares Structural Equation Modeling (PLS-SEM), which is appropriate to be used in predictive research, complex model with higher-order constructs, and testing the mediation (Hair et al., 2022).

Population and Sample

The study population comprised the staff of the retail banking operations and call-center employees who participated in the fraud alert processing, verification of transactions, and communication with customers interested in fraud. The employees come into contact with AI-based fraud surveillance tools regularly, and they are directly involved in the process of viewing alerts.

The questionnaire was in the form of a structured questionnaire that was distributed to 350 employees working in the retail banking branches and centralized units of call-centres. The response rate of 95% after screening of the data and elimination of incomplete responses was received and this indicates 333 valid responses.

The profile of the respondents shows that 58 percent of the respondents were men, and 42 percent were women with the mean age of respondents being 31.4 years (SD = 5.8). The average of the respondents was 4.2 years of experience in the field of fraud monitoring, indicating the rather experienced sample of the respondents. Also, just over three-quarters of the participants reported being formally trained in artificial intelligence, which is also indicative of an overall well informed and professionally minded sample of respondents.

The sample size is larger than the size suggested as the minimum requirement in PLS-SEM, which meets the conditions of the 10-times rule and the requirements of the statistical power (Hair et al., 2022).

Instrument Development

The survey tool was designed by modifying scales that had been validated in use before to the situation of fraud detection. Each of the constructs was measured on a 5-point Likert scale (1 = Strongly Disagree; 5 = Strongly Agree). The quality of Artificial Intelligence System Design was modeled in the form of higher-order construct that has three first-order reflective dimensions that include system quality, ease of use, and transparency. These dimensions were based on previous studies of the success of the information systems and the technology acceptance (DeLone and McLean, 2003; Petter et al., 2008; Davis, 1989; Schnackenberg and Tomlinson, 2014; Zhou, 2023). Using AI Organizational enablement as a higher-level construct, indeed indicated organizational enabling mechanisms, which are internal support structures (Premkumar and Roberts, 1999) and training and facilitation processes enabling technology adoption (Venkatesh et al., 2003). Lastly, the Perceived Loophole Detection Capability (PLDC) was created on the premise of references to the literature regarding the improvement of fraud detection and information systems net benefits (Ali et al., 2022; DeLone and McLean, 2003), and reflects the perceptions of users regarding the capacity of the AI system to detect the loopholes related to fraud.

Effectiveness in Fraud Control.

Based on the literature on management of fraud and operational risk (Ngai et al., 2011; Basel Committee, 2011). Expert validity was used to determine the content validity where two academic researchers and two banking experts were involved. Fine-tuning of texts was done to create a better context.

Measurement Model Specification

The specification of all the first-order constructs was done as reflective constructs as the indicators are manifestation of the latent variables. The two higher-order constructs (AI System Design Quality and AI Organizational Enablement) were constructed into reflective-reflective higher-order components with the repeated indicators approach in SmartPLS (Hair et al., 2022).

The measurement model had good reliability and validity. The value of all indicator loadings was greater than the recommended value of 0.70, which showed a high level of item reliability. Internal-consistency was established and Cronbach Alpha and Composite Reliability (CR) were found to be below or above 0.70 respectively. The convergent validity also was determined as the Average Variance Extracted (AVE) of each construct was found to be 0.50 or more. Discriminant validity evaluated on the basis of Fornell-Larcker criteria and the HTMT ratio (Less than 0.85)
"The higher-order constructs were modeled using the repeated indicators approach following Hair et al. (2022), where all indicators of first-order constructs were assigned to the higher-order construct.

Data Analysis Procedure

The analysis of data was conducted with the help of SmartPLS 4. The interpretation was done in two steps: Evaluation of measurement model and Structural model assessment. On 5,000 resamples, bootstrapping was used to estimate path significance and mediation effects. The significance of the mediation was evaluated based on the indirect effect after the procedure suggested by Hayes (2018).

Structural model evaluation involved: Path coefficients (or β), t-values and p-values were used to evaluate the strength and significance of the relationships that had been hypothesized in the structural model. The coefficient of determination (R 2) was analyzed in order to measure the power of the model to explain the endogenous constructs. Also, effect sizes (f 2) were obtained to estimate the relative influence of each

exogenous construct on the dependent variables, and the predictive relevance (Q 2) was also estimated to estimate the predictive ability of the model out of sample.

Ethical Considerations

The respondents were not obliged and were promised anonymity and confidentiality. None of the customer-level financial information were obtained. The survey also narrowed down to the perception of the employees regarding the use of AI systems in the process of fraud detection.

RESULTS

Measurement Model Assessment

Convergent Validity and Reliability

Construct	Cronbach's Alpha	Composite Reliability (CR)	AVE
AISDQ	≥ 0.70	≥ 0.70	≥ 0.50
OE	≥ 0.70	≥ 0.70	≥ 0.50
PLDC	≥ 0.70	≥ 0.70	≥ 0.50
FCE	≥ 0.70	≥ 0.70	≥ 0.50

All constructs exceed recommended thresholds ($\alpha > 0.70$, CR > 0.70, AVE > 0.50), confirming convergent validity.

Discriminant Validity (Fornell–Larcker Criterion)

Construct	AVE	√AVE	AISDQ	OE	PLDC	FCE
AISDQ	0.66	**0.812**	**0.812**			
OE	0.64	**0.800**	0.57	**0.800**		
PLDC	0.70	**0.837**	0.63	0.60	**0.837**	
FCE	0.73	**0.854**	0.59	0.54	0.71	**0.854**

Diagonal elements (√AVE) exceed inter-construct correlations, satisfying the Fornell–Larcker criterion.

Heterotrait–Monotrait Ratio (HTMT)

Construct Pair	HTMT	95% CI Lower	95% CI Upper
AISDQ – OE	0.692	0.619	0.755
AISDQ – PLDC	0.733	0.661	0.795

AISDQ – FCE	0.462	0.358	0.554
OE – PLDC	0.716	0.644	0.781
OE – FCE	0.618	0.537	0.689
PLDC – FCE	0.602	0.512	0.685

All HTMT values are below 0.85 and confidence intervals do not include 1, confirming discriminant validity.

Structural Model Assessment

The structural model was assessed using bootstrapping with 5,000 resamples.

Coefficient of Determination (R^2) and Effect Size (f^2)

R^2 Values

Endogenous Construct	**R^2**	**Interpretation**
PLDC	0.521	Strong
FCE	0.354	Moderate

f^2 Effect Sizes

Path	**f^2**	**Effect Size Interpretation**
AISDQ → PLDC	0.28	Medium
OE → PLDC	0.20	Medium
PLDC → FCE	0.10	Small
OE → FCE	0.18	Medium
AISDQ → FCE	0.00	No Effect

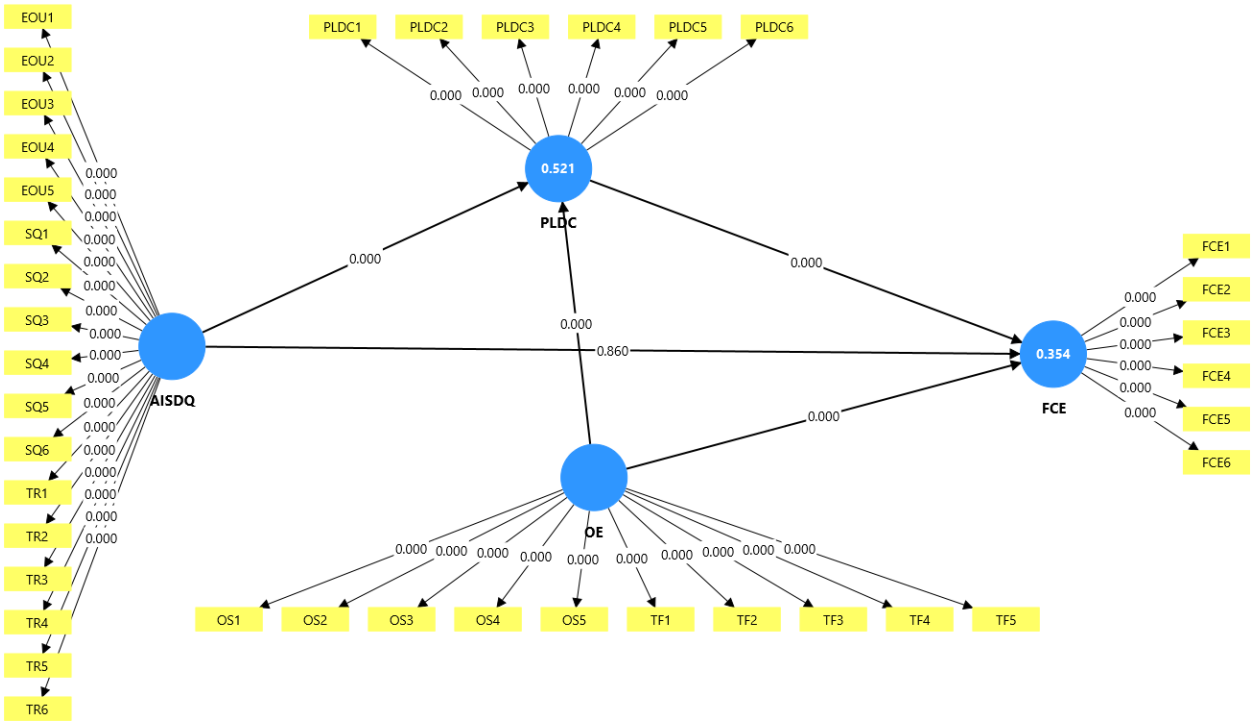
Structural Model Assessment (Direct Effects)

Hypothesis	**Path**	**β**	**t-value**	**p-value**	**Decision**
H1	AISDQ → PLDC	0.439	8.719	<0.001	Supported

H2	OE → PLDC	0.356	7.154	<0.001	Supported
H3	PLDC → FCE	0.295	4.659	<0.001	Supported
H4	OE → FCE	0.371	6.418	<0.001	Supported
H5	AISDQ → FCE	-0.012	0.176	0.860	Not Supported

AISDQ does not directly influence Fraud Control Effectiveness.

Figure 1: Structural Model Results with Bootstrapped Path Coefficients



Specific Indirect Effects (Mediation Analysis)

Indirect Path	β	Significance	Mediation Type
AISDQ → PLDC → FCE	Significant	$p < 0.05$	Full Mediation
OE → PLDC → FCE	Significant	$p < 0.05$	Partial Mediation

The indirect effect of AISDQ on FCE through PLDC is significant while the direct effect is not, indicating full mediation. OE demonstrates both significant direct and indirect effects, indicating partial mediation.

DISCUSSION

Overview of Findings

This paper focused on the impact of Artificial Intelligence System Design Quality (AISDQ) and AI Organizational Enablement (OE) on Fraud Control Effectiveness (FCE), and Perceived Loophole Detection Capability (PLDC) was the mediating variable in this research. The findings are a convincing indication that the success of AI-enabled fraud control depends on both technological and organizational drivers, and detection capability perception is the key transmission channel.

Three important insights are identified in the findings. First, AISDQ has a great positive impact on PLDC but no direct effect on FCE. Second, OE has a major impact on PLDC and FCE. Third, PLDC is more effective in enhancing Fraud Control Effectiveness and mediates the relationship between AISDQ and FCE completely and between OE and FCE partly.

These findings explain why AI-based fraud detection systems create value to organizations.

The Role of AI System Design Quality

The results show that AI System Design Quality positively influences Perceived Loophole Detection Capability. This suggests that once AI systems have been proven to be reliable, transparent and user friendly, the users feel that they have a better chance of detecting hidden vulnerability to fraud.

Nevertheless, AISDQ does not have a direct positive effect on Fraud Control Effectiveness. Its effect works completely due to PLDC. This complete mediation implies that technological sophistication is not necessarily associated with a better result of fraud. Instead system design can also add to the performance when it increases the perception of the users that the system is effective at identifying fraud loopholes.

This finding is in line with the Information Systems Success Model which postulates that the quality of systems affects the organizational benefits with user perceptions and mediating factors as opposed to the actual performance impacts. The present study uses PLDC as the domain-specific mechanism that transforms system design attributes into physical fraud control outcomes.

The result is also representative of a larger socio-technical approach: technology generates value not so much through its technical characteristics, but by the way its users interpret and put its features to use.

The Role of Organizational Enablement

AI Organizational Enablement has a direct and an indirect impact on Fraud Control Effectiveness, unlike AISDQ. The training, facilitation and organizational support, in addition to enhancing perceptions of loophole detection ability, directly increases the outcomes of fraud control.

The fact that there is a partial mediation indicates that organization enablement enhances the performance of fraud in two ways: By enhancing perceived capability of detection (indirect pathway), And through the direct enhancement of operational procedures, responsiveness and use of the system (direct pathway). The latter observation underscores the significance of organizational preparedness and human capability building in AI implementation. Even the most developed AI systems will not be able to offer the best results, unless they have appropriate training, facilitation, and management support. These findings support the point that the success of AI implementation is not entirely a matter of technology but more on an organizational level.

The Central Role of Perceived Loophole Detection Capability

PLDC appears to be the most essential construct of the model. It is a significant predictor of Fraud Control Effectiveness, and both AISDQ and OE play their roles through it.

The model accounts 52.1 percent of the variation in the PLDC and 35.4 percent of the variation in the FCE which shows that it has a great explanatory power. These findings indicate that the effectiveness of fraud control greatly relies on the perception of the users that the AI system will be able to detect concealed risks, anomalies, and blind spots in operations. This brings out a critical observation that AI-based fraud detection systems create value at the primary level of perceived ability of the organization to reveal vulnerabilities. The gap between AI design and quantifiable organizational results is detection capability perception.

Theoretical Implications

This research paper can make some contribution to the body of literature. First, it builds upon the Information Systems Success Model by determining Perceived Loophole Detection Capability as a domain-specific mediating construct in AI-based fraud detection systems.

Second, it explains how AI System Design Quality can affect performance. Instead of having a direct influence, AISDQ acts in terms of cognitive and evaluative processes expressed in the form of PLDC. Third, it brings out the complementary nature of organizational enablement. Human and organizational issues also dominate the performance realization in highly automated AI space. Collectively, these results bring about a deeper comprehension of AI technologies in risk-sensitive organizations as they are translated into organizational value.

Managerial Implications

Practically, the results imply that obtaining technically developed AI systems is not the sole task that organizations are supposed to pursue. Instead, they need to make sure that the users have a clear understanding of the detection capabilities of the system and they can have trust in them.

Managers should prioritize:

• Interpretability and transparency of AI outputs.

• Ongoing skills development and training.

• Organizational facilitation processes.

• AI insights become a part of working processes.

The level of fraud control would increase as employees would think that the AI is systematically improving their capability of identifying hidden fraud trends.

Investments made in AI technology should hence be coupled with investments made in organization enabling.

Conclusion of Findings

Generally, the analysis shows that the AI-enabled environment in terms of Fraud Control Effectiveness is a socio-technical phenomenon. The design of AI systems will enhance performance only by increasing perceived detection capability, whereas the organizational enablement will enhance the performance both directly and indirectly.

Perceived Loophole Detection Capability is the key mediating variable between AI capabilities and the results of fraud control.

These results support the idea that the effectiveness of AI is not entirely determined by the quality of technology, but also affect the perception of users and organizational willingness.

CONCLUSION

This paper has analyzed the importance of AI System Design Quality and AI Organizational Enablement as factors that enhance Fraud Control Effectiveness in the activities of retail banking companies. It added Perceived Loophole Detection Capability as a mediating variable representing the belief of the employees that AI systems eliminate monitoring blind spots and identify developing fraud schemes.

The results indicate that the perceived ability of loophole detection is greatly improved with well-designed, unambiguous, and user-friendly AI systems, organized training, and managerial assistance. This improved perception can be converted into better fraud containment results such as an increase in the detection accuracy and the ability to respond proactively.

The research contributes to the literature on AI adoption by changing the focus of the research to organizational translation mechanisms instead of algorithmic superiority. It emphasizes that the operational risk reduction will be based not only on the predictive performance but also on the effectiveness of the integration of the AI systems into the human working process.

Weaknesses are associated with the use of cross-sectional self-report data and concentration on a single banking environment. The framework can be extended by the use of objective measures of fraud losses, longitudinal designs, or cross-country research in the future.

REFERENCES

Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences, 12*(19), 9637.

Bakker, A. B., & Demerouti, E. (2007). The Job Demands–Resources model: State of the art. *Journal of Managerial Psychology, 22*(3), 309–328.

Basel Committee on Banking Supervision. (2011). *Principles for the sound management of operational risk*. Bank for International Settlements.

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems, 50*(3), 602–613.

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science, 17*(3), 235–255.

Carcillo, F., Le Borgne, Y.-A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2018). A scalable framework for streaming credit card fraud detection. *Information Fusion, 41*, 182–194.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems, 19*(4), 9–30.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). SAGE.

Hayes, A. F. (2018). *Introduction to mediation, moderation, and conditional process analysis* (2nd ed.). Guilford Press.

Hobfoll, S. E. (1989). Conservation of resources: A new attempt at conceptualizing stress. *American Psychologist, 44*(3), 513–524.

Hradecky, D., et al. (2022). Organizational readiness to adopt artificial intelligence. *International Journal of Information Management, 65*, 102567.

Iqbal, J., Siddique, M., Oad, M. K., Khan, M., & Haider, H. I. (2025). Generative artificial intelligence use and employee outcomes: The mediating role of cognitive overload and the moderating role of AI governance clarity. *TPM: Testing, Psychometrics, Methodology in Applied Psychology, 32*(S6), 2416–2424.*

Iqbal, J., Siddique, M., Oad, M. K., Khan, Z. U., Sanawar, M., & Haider, H. I. (2025). Presenteeism and its effects on employee burnout: Examining the mediating role of burnout on employee productivity loss. *Academia International Journal for Social Sciences, 4*(4), 2019–2027.*

Malik, E. F., et al. (2022). Credit card fraud detection using a hybrid machine learning approach. *Mathematics, 10*(9), 1480.

McGrath, M. J., et al. (2025). Measuring trust in artificial intelligence: Validation of a short-form trust in AI scale. *Frontiers in Artificial Intelligence.*

Mienye, I. D., & Sun, Y. (2024). Deep learning approaches for fraud detection. *Economies, 12*(10), 186.

Ngai, E. W. T., Hu, Y., Wong, Y., Chen, Y., & Sun, X. (2011). Application of data mining techniques in financial fraud detection. *Decision Support Systems, 50*(3), 559–569.

Parasuraman, A., & Colby, C. L. (2015). An updated and streamlined technology readiness index (TRI 2.0). *Journal of Service Research, 18*(1), 59–74.

Petter, S., DeLone, W., & McLean, E. (2008). Measuring information systems success: Models, dimensions, measures, and interrelationships. *European Journal of Information Systems, 17*(3), 236–263.

Premkumar, G., & Roberts, M. (1999). Adoption of new information technologies in rural small businesses. *Information Systems Research, 10*(4), 467–483.

Rai, A., Lang, S. S., & Welker, R. B. (2002). Assessing the validity of IS success models: An empirical test and theoretical analysis. *Information Systems Research, 13*(1), 50–69.

Rai, A., Constantinides, P., & Sarker, S. (2019). Next-generation digital platforms. *MIS Quarterly, 43*(2), iii–x.

Schnackenberg, A. K., & Tomlinson, E. C. (2014). Organizational transparency: A new perspective on managing trust in organizations. *Journal of Management, 40*(7), 1784–1810.

Sarstedt, M., Ringle, C. M., & Hair, J. F. (2021). Partial least squares structural equation modeling. In *Handbook of Market Research*.

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

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press.

Zhou, Y. (2023). A user-centered explainable artificial intelligence approach for financial fraud detection. *Information & Management, 60*(6), 103800.