International Journal of Finance and Managerial Accounting, Vol.12, No.47, Autumn 2027 IJFMA

# The Impact of Artificial Intelligence Algorithms on Financial Fraud Detection and Prevention: The Moderating Role of Internal Control Systems

**Amir.Ansari**
Department of Accounting, Yas.C., Islamic Azad University, Yasuj, Iran

**Hashem Valipour**
Department of Accounting, Fir.C., Islamic Azad University, Firuzabad, Iran
(Corresponding Author)

**Hamid Salehi**
Department of Accounting, Fir.C., Islamic Azad University, Firuzabad, Iran.

**Submit: 22/06/2025 Accept: 10/09/2025**

## ABSTRACT

This study rigorously examines the influence of artificial intelligence (AI) algorithms on the detection and prevention of financial fraud, with a particular emphasis on the moderating role of internal control systems. Utilizing a quantitative, applied research design with a descriptive-survey approach, data were collected from 150 professionals across the domains of finance, auditing, information technology, and risk management through validated questionnaires administered via both online and offline channels.

The research evaluates the efficacy of advanced AI techniques—including machine learning models, natural language processing (NLP), graph-based analytics, and real-time detection systems—in identifying intricate, non-obvious, and evolving fraudulent financial behaviors. The findings reveal that the integration of AI technologies significantly enhances fraud detection accuracy and responsiveness. Crucially, this positive impact is markedly amplified in organizational environments characterized by robust, well-structured internal control mechanisms.

The results underscore the synergistic interplay between technological innovation and governance infrastructure, indicating that effective internal controls serve as a critical enabler in maximizing the potential of AI for financial fraud risk mitigation. This study contributes a novel empirical and conceptual framework that informs both academic inquiry and managerial practice, offering strategic insights for organizations aiming to enhance the resilience and intelligence of their financial oversight systems.

## Keywords:

Intelligent Financial Monitoring, Fraud Detection Algorithms, Effective Internal Control, Language and Graph Analytics, Real-time Anomaly Detection.

## 1. Introduction

Financial fraud remains a persistent and significant threat to the credibility and stability of global financial systems. Beyond causing substantial economic losses, fraud undermines investor confidence, distorts market efficiency, and weakens the integrity of corporate governance frameworks (Button, Johnston, & Frimpong, 2007). According to the Association of Certified Fraud Examiners (ACFE, 2022), organizations lose approximately 5% of their annual revenue to fraud, underscoring the urgent need for more robust and proactive detection mechanisms.

Traditional fraud detection methods—including manual audits, internal reviews, and rule-based systems—are increasingly inadequate in addressing the complexity and scale of modern fraud schemes. These methods struggle to process large volumes of real-time transactional and behavioral data, and are limited in detecting non-linear, adaptive, and concealed fraud patterns (Ngai et al., 2011). In response, there has been a growing shift toward the use of artificial intelligence (AI) and machine learning (ML) technologies, which offer enhanced speed, accuracy, and predictive capabilities in fraud detection (West & Bhattacharya, 2016).

AI-based approaches—such as neural networks, support vector machines (SVM), decision trees, and deep learning—are capable of analyzing massive datasets to uncover hidden patterns and anomalies indicative of fraudulent behavior (Zhou, Han, & Zhang, 2018). Techniques like natural language processing (NLP) can extract insights from unstructured text, including financial statements and contracts, while graph analytics enables the mapping and monitoring of complex transactional networks (Bai, Zhou, & Wang, 2021). These capabilities have begun transforming fraud detection practices across the banking, insurance, and e-commerce sectors.

However, the effectiveness of AI in fraud detection is not solely dependent on technological sophistication. Internal control systems play a critical role in enabling or constraining the impact of AI technologies (Murphy & Free, 2016). Effective internal controls—comprising risk assessments, control activities, information systems, communication channels, and monitoring mechanisms—are essential to ensure data integrity, compliance, and ethical conduct (COSO, 2013). When internal controls are weak or fragmented, AI systems may operate on incomplete or inaccurate data, leading to false positives, undetected fraud, and increased compliance risks (Mohammadrezaei, Lee, & Deng, 2021).

This interdependence is particularly salient in emerging economies such as Iran, where financial systems often face institutional weaknesses, governance challenges, and inconsistent regulatory enforcement (Hassan, Qiang, & Khan, 2020). As Iran's financial sector undergoes rapid digital transformation, the deployment of AI-driven risk management tools presents both opportunities and challenges. Without concurrent improvements in internal control infrastructure, these advanced technologies may yield limited results or introduce new vulnerabilities (Salehi, Zarei, & Moradi, 2021). Recent literature highlights that the success of AI in fraud detection is highly contingent upon the strength of organizational controls, data governance, and compliance mechanisms (Lamba, 2019).

Despite increasing academic and industry attention to AI applications in fraud management, a significant empirical gap remains concerning how internal control systems interact with AI technologies in real-world settings—especially in contexts characterized by regulatory uncertainty and institutional fragility. This study aims to address this gap by empirically investigating the direct impact of AI algorithms on financial fraud detection and examining the moderating role of internal control effectiveness. Drawing from information systems, accounting, and organizational control theories, this research develops a contextually grounded framework to enhance fraud detection in developing financial environments (Abbasi, Albrecht, Vance, & Hansen, 2012; Appelbaum, Kogan, & Vasarhelyi, 2017). The findings aim to provide actionable insights for policymakers, auditors, and financial institutions seeking to balance technological innovation with robust governance and oversight.

## 2. Theoretical Foundations and Research Hypotheses

Financial fraud represents a multidimensional and evolving challenge that continues to undermine the foundational pillars of global financial stability. It not only erodes market integrity and investor trust but also distorts capital allocation, misprices risk, and contributes to systemic vulnerabilities (Pham et al.,

2021). According to the Association of Certified Fraud Examiners (ACFE, 2022), organizations worldwide lose an estimated 5% of their annual revenues due to fraudulent activities. These risks are often magnified in developing economies, where institutional fragility, weak regulatory enforcement, and inadequate governance structures create conducive environments for fraudulent behavior.

In today's high-volume, high-velocity data landscape, traditional fraud detection mechanisms—such as random sampling, manual audits, and rule-based systems—are increasingly inadequate. These methods struggle to identify complex, non-linear fraud patterns embedded in dynamic financial data. As a result, organizations are turning to artificial intelligence (AI), particularly machine learning (ML) models, which offer scalable, adaptive, and data-driven capabilities. Algorithms such as deep neural networks, random forests, and support vector machines (SVMs) can extract hidden patterns and make probabilistic inferences from both structured and unstructured financial data streams (Liu & Li, 2022; Brown et al., 2023).

However, the successful application of AI in fraud detection is not solely dependent on algorithmic sophistication. Internal control systems play a crucial moderating and enabling role in ensuring that AI produces meaningful fraud mitigation outcomes. Empirical evidence suggests that organizations with robust internal controls—encompassing governance protocols, risk oversight mechanisms, audit processes, and ethical control environments—are better equipped to leverage AI technologies effectively (Pravit et al., 2021). Strong internal controls not only enhance data integrity but also provide the organizational context necessary to interpret AI-driven insights and implement timely corrective actions (Chen et al., 2020).

This interaction between AI capabilities and internal control effectiveness is particularly salient in emerging markets such as Iran, where rapid financial digitalization is unfolding amidst underdeveloped institutional frameworks. While Iranian financial institutions increasingly embrace digitization, the relative absence of strong internal controls, corporate transparency, and rule-of-law enforcement heightens the risk of undetected fraud and algorithmic error (Transparency International, 2024). In such environments, an over-reliance on technology without corresponding organizational readiness may lead to unintended consequences, including biased decision-making and regulatory non-compliance.

To address these challenges, the present study draws on a set of theoretical frameworks that conceptualize the co-evolution of technology and institutional structures in shaping organizational outcomes. These include Organizational Information Processing Theory (Galbraith, 1973, 1974), which emphasizes the alignment between information processing capabilities and environmental uncertainty; Real-Time Organizational Response Theory (Vick & Sutcliffe, 2001), which highlights the importance of time-sensitive decision support systems; the Technology-Organization-Environment (TOE) framework (Tornatzky & Fleischer, 1990), which underscores the influence of internal and external factors on technological adoption; and Social Network and Graph Theories, which provide tools for mapping and analyzing complex inter-entity relationships.

These theoretical lenses inform the central premise of this study: that the effectiveness of AI in financial fraud detection depends not only on the sophistication of the technology itself but also on the institutional and procedural architecture that supports, regulates, and interprets it. The subsequent sections of this paper develop hypotheses grounded in these theoretical foundations and explore the interplay between AI-based fraud detection systems and internal control mechanisms within the specific institutional context of Iran.

## 2.1 Machine Learning Algorithms and Fraud Pattern Recognition

Organizational Information Processing Theory (OIPT) posits that in environments characterized by uncertainty and complexity, organizations must enhance their information processing capacities to make accurate and timely decisions (Galbraith, 1973). In the context of financial fraud detection, machine learning (ML) algorithms—including deep neural networks, support vector machines (SVMs), and decision trees—address this need by uncovering complex, non-linear fraud patterns that are often imperceptible to traditional analytical methods (Brown et al., 2023). However, the effectiveness of these algorithms is closely tied to the quality of the organizational environment in which they operate.

Robust internal control systems improve data integrity, minimize informational noise, and provide oversight mechanisms that support the training, interpretability, and reliability of ML models (Pravit et al., 2021).

**Hypothesis 1**: The strength and effectiveness of internal control systems positively and significantly moderate the relationship between the application of machine learning algorithms and the accuracy of detecting complex and atypical financial fraud patterns.

## 2.2 Real-Time Organizational Response Theory and Fraud Detection Speed

Real-Time Organizational Response Theory emphasizes the importance of continuous monitoring and rapid response in volatile and high-risk operational environments (Vick & Sutcliffe, 2001). In fraud detection, artificial intelligence systems equipped with real-time analytics capabilities can identify anomalies as they occur, allowing organizations to act before losses escalate. Nevertheless, the translation of real-time insights into actionable interventions depends heavily on the presence of well-structured internal controls—such as clearly defined escalation protocols, efficient communication channels, and standardized documentation practices (Chen et al., 2020). Without these organizational mechanisms, the speed advantage of real-time analytics may be neutralized by delays or inefficiencies in decision-making and follow-up actions.

**Hypothesis 2**: The strength and effectiveness of internal control systems positively and significantly moderate the relationship between the use of AI-enabled real-time analytics and the accuracy of detecting complex and atypical financial fraud patterns.

## 2.3 Linguistic Cues Theory and Natural Language Processing

The Linguistic Cues Theory of Fraud suggests that deceptive financial communications often manifest unique language features—such as abstract wording, emotional inconsistency, and avoidance of specific details—that can serve as indicators of fraud (Humphries et al., 2023). Natural language processing (NLP) and sentiment analysis techniques enable the automated detection of such cues across various unstructured data sources, including annual reports, earnings calls, and internal communications. However, the utility of these tools depends on the organization's capacity to validate textual outputs, triangulate interpretations with other data sources, and apply corrective governance responses. Effective internal controls facilitate this process by ensuring consistency, accountability, and alignment with risk management frameworks.

**Hypothesis 3**: The strength and effectiveness of internal control systems positively and significantly moderate the relationship between the use of NLP and sentiment analysis techniques and the accuracy of detecting complex and atypical financial fraud patterns.

## 2.4. Graph Analysis and the Detection of Concealed Fraud Networks

Social Network Theory and graph-based analytics suggest that fraudulent activities such as collusion, insider trading, and money laundering are often embedded within complex and opaque relational structures that traditional detection methods are ill-equipped to identify (Zhao et al., 2023). AI-powered graph analytics allow organizations to map and interrogate these concealed relationships by analyzing connections among individuals, entities, and transactions across large and multidimensional datasets. These tools enable the identification of network-level anomalies and hidden clusters indicative of fraudulent behavior.

However, the effectiveness of graph-based fraud detection is highly contingent upon the integrity of the underlying data and the organizational mechanisms that support the interpretation of analytical outputs. Weak internal controls can result in incomplete or inaccurate data mapping, while the absence of structured response protocols may undermine the utility of the insights generated. Conversely, strong internal controls—comprising robust data governance, clear role delineation, and monitoring procedures—facilitate the contextualization, validation, and operationalization of AI-generated fraud signals.

**Hypothesis 4**: The strength and effectiveness of internal control systems positively and significantly moderate the relationship between the use of graph-based AI techniques and the accuracy of detecting complex and concealed financial fraud patterns.

## 2.5 Integrating AI with Internal Controls: The Role of the TOE Framework

The integration of AI capabilities within strong internal control environments presents a promising pathway toward more proactive and precise fraud detection. The Technology–Organization–Environment (TOE) framework emphasizes that the successful implementation of technological innovation depends not only on the technology itself, but also on the organization's internal readiness and its alignment with the surrounding institutional environment (Tornatzky & Fleischer, 1990). In this regard, AI applications must be supported by governance structures, risk management protocols, and organizational culture to generate meaningful outcomes.

This alignment is particularly critical in fragile institutional contexts such as Iran, where regulatory enforcement remains inconsistent, corporate transparency is limited, and systemic corruption poses persistent challenges (Transparency International, 2024). In such environments, the uncritical deployment of AI systems—without the parallel development of internal control capabilities—may not only limit detection efficacy but could also introduce new forms of technological and ethical risk.

Therefore, this study poses the following central research question:

**To what extent does the strength and effectiveness of internal control systems moderate the relationship between AI adoption and the efficacy of financial fraud detection and prevention?**

By exploring this question, the research aims to develop a theoretically grounded, empirically tested, and practically actionable framework that informs both organizational strategies and regulatory policymaking in high-risk, data-intensive environments

# 3.Literature Review

The integration of artificial intelligence (AI) into financial fraud detection has become a pivotal focus in both academic research and applied financial analytics. Over the past decade, numerous studies have highlighted the capabilities of advanced AI techniques—particularly machine learning (ML), natural language processing (NLP), and graph-based analytics—in uncovering complex, concealed, and evolving fraudulent patterns (Ngai et al., 2011; West & Bhattacharya, 2016). These techniques offer significant technical advantages, but their practical effectiveness is heavily influenced by the institutional infrastructure, notably the strength of internal control systems (Chen et al., 2020).

## 3.1.AI Applications in the Iranian Financial Context

Several empirical studies from Iran demonstrate the potential of AI-driven fraud detection models. For example, Zarei et al. (2026) applied Support Vector Machine (SVM) algorithms to data from 136 listed companies (2016–2022), achieving an accuracy of 85% alongside high recall and precision rates. Similarly, Nikbakht and Panahi (2023) reported that a hybrid approach combining neural networks with variable selection techniques produced an accuracy of 82% when applied to Tehran Stock Exchange firms. Maleki Kaklar et al. (2021) also showed that hybrid decision-tree models outperform traditional statistical methods in fraud detection accuracy. These findings collectively confirm the efficacy of AI techniques in the Iranian market and support the relevance of hybrid modeling approaches. From a conceptual standpoint, Sarraf and Farghian (2022) emphasized the importance of integrating expert systems and fuzzy logic to enhance automation and fraud resilience.

## 3.2.International Evidence on AI and Internal Controls

At the global level, research consistently highlights that the success of AI in fraud detection depends not only on algorithmic sophistication but also on the maturity of internal controls. Fam, Li, and Tran (2021) performed a meta-analysis illustrating the high detection capabilities of models like Random Forest and Deep Neural Networks, while underscoring risks such as algorithmic drift and bias in weak control environments. Chen, Li, and Prawitt (2020) further confirmed that organizations with robust internal control systems experience fewer detection errors and greater predictive accuracy.

## 3.3.Linguistic and Network-based Fraud Detection

Linguistic analysis through NLP offers another promising avenue for fraud detection. Humphries, Perez, and Kumar (2023) identified stylistic markers of

deception, yet stressed the necessity of expert validation and internal monitoring to ensure reliability (Goel et al., 2010). In parallel, Brown, Smith, and Wang (2023) demonstrated the enhanced efficacy of combining ML with graph analytics for uncovering complex fraud networks, noting that strong internal controls are essential for data integrity and interpretive transparency. Zhao, Zhang, and Liu (2023) similarly highlighted the dependency of graph-based models on sound data governance, and Nguyen, Zhao, and Patel (2024) reported increased algorithmic risks in digital banking systems with weak internal controls.

### 3.4.Synthesis and Research Gap

Taken together, the literature presents a coherent narrative: AI holds transformative potential for financial fraud detection, but this potential is conditional upon the robustness of internal control systems (COSO, 2013; Murphy & Free, 2016). Internal controls validate data quality and provide the procedural frameworks required to convert AI outputs into actionable, compliant decisions. However, while prior studies have separately examined AI technologies and internal controls, fewer investigations have explored their interactive effects, especially within emerging markets. This gap underscores the need for research—such as the present study—that investigates how internal controls moderate the effectiveness of AI in fraud detection within risk-prone financial environments.

## 4.Research Methodology

This study adopts an applied and empirical orientation, aimed at generating actionable insights into how artificial intelligence (AI) integration—when supported by robust internal control systems—can enhance the detection of financial fraud. Methodologically, the research employs a quantitative, descriptive-survey design, well-suited for examining relationships among latent constructs within real-world organizational contexts.

The target population comprises domain professionals—financial analysts, auditors, IT specialists, and risk managers—employed across major public and private sector organizations in Iran. These individuals were selected due to their direct involvement in fraud detection processes and the design, implementation, or oversight of internal controls. To ensure the representativeness of the sample across occupational strata, a stratified proportional sampling method was employed. Following Krejcie and Morgan's (1970) sample size determination table for large populations, a minimum threshold of 150 responses was deemed statistically sufficient. Final data collection was conducted through both digital (online) and physical (on-site) methods to maximize respondent diversity and mitigate selection bias.

Data were gathered using a structured and pilot-tested questionnaire comprising 40 items, categorized into two core dimensions:

1. The extent and effectiveness of AI deployment in financial fraud detection; and
2. The comprehensiveness and maturity of internal control systems.

The questionnaire was developed based on established measurement models and constructs from previous validated studies (Ngai et al., 2011; Akoglu et al., 2015; Abdullah et al., 2016; Abri & Mohammadi, 2024). All items were measured using a five-point Likert scale (1 = strongly disagree to 5 = strongly agree), in line with psychometric conventions for evaluating perceptual and behavioral constructs.

Content validity was established through expert panel reviews to ensure that the measurement items aligned with internationally recognized frameworks, particularly the COSO 2013 Integrated Framework. The internal control strength construct was operationalized based on the five dimensions of the COSO framework: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. Each dimension was measured using multiple items adapted from validated scales to comprehensively capture the multifaceted nature of internal controls.

To assess the reliability of the constructs, Cronbach's alpha coefficients were calculated for each COSO dimension and the overall internal control construct, all exceeding the recommended threshold of 0.70, indicating satisfactory internal consistency. Furthermore, Composite Reliability (CR) and Average Variance Extracted (AVE) were computed, confirming both convergent validity and construct validity of the measurement model

Data analysis was performed using SPSS version 26 and SmartPLS version 4. Descriptive statistics were first used to profile the sample and assess response

distribution. To validate the measurement model, Confirmatory Factor Analysis (CFA) was applied, using the Fornell–Larcker criterion to test discriminant validity and factor loadings/AVE to evaluate construct reliability. For testing structural relationships, Partial Least Squares Structural Equation Modeling (PLS-SEM) was employed—an approach appropriate for complex models involving latent variables, limited sample sizes, and non-normal distributions (Hair et al., 2019).

Beyond basic path analysis, the study conducted interaction modeling and multi-group analysis to assess the moderating role of internal control strength on the relationship between AI utilization and fraud detection performance. Significance levels were tested through bootstrapping with 5,000 resamples, generating empirical p-values and confidence intervals to validate model robustness.

This comprehensive methodological approach not only enhances the validity and generalizability of the findings but also provides a rigorous empirical basis for theoretical advancement and managerial decision-making in data-intensive and high-risk financial environments

# 5. Research Findings

## 5.1 Analysis and Interpretation of Demographic Data

Table 1 outlines the demographic characteristics of the 150 professionals who participated in the study. The age distribution reveals that the most represented cohort falls within the 31–40 age range (37.3%), indicative of a dominant mid-career professional group likely to possess operational and strategic insight into organizational processes. Participants aged 41–50 make up 25.3%, further highlighting the experience-rich nature of the sample. In contrast, respondents aged over 50 represent the smallest group (14.7%), suggesting limited representation from upper executive or senior advisory roles.

Gender distribution reflects a notable skew, with male respondents comprising 61.3% of the sample compared to 38.7% female. This discrepancy underscores the persistent gender imbalance in the domains of finance, auditing, and information systems in the Iranian professional context, consistent with broader regional labor trends.

Regarding professional tenure, a plurality of respondents (32.0%) possess 6–10 years of experience, followed by 28.0% with 11–15 years and 22.7% with more than 15 years of experience. This composition ensures that insights are drawn from individuals with meaningful exposure to real-world fraud detection and internal control operations, adding depth and credibility to the dataset.

From an educational standpoint, 56.0% of respondents hold a Master's degree, 26.0% possess a Bachelor's degree, and 18.0% hold a Doctorate. The high proportion of postgraduate qualifications reflects a technically competent and academically informed respondent pool, capable of providing nuanced evaluations of advanced technologies such as AI and their institutional contexts.

In terms of domain specialization, finance (34.0%) and auditing (28.7%) dominate, directly aligning with the research's core focus. Information technology specialists account for 21.3%, ensuring that technical perspectives on AI deployment are well-represented. The remaining 16.0% categorized as "other" encompass auxiliary functions such as compliance, legal advisory, and risk analysis, contributing to a multidimensional understanding of fraud detection practices.

**Table 1: Demographic Information of Respondents**

| Variable | Category | Frequency | Percentage (%) |
|---|---|---|---|
| Age | Under 30 years | 34 | 22.7 |
| | 31–40 years | 56 | 37.3 |
| | 41–50 years | 38 | 25.3 |
| | Over 50 years | 22 | 14.7 |
| Gender | Male | 92 | 61.3 |
| | Female | 58 | 38.7 |
| Work Experience | Under 5 years | 26 | 17.3 |
| | 6–10 years | 48 | 32.0 |
| | 11–15 years | 42 | 28.0 |
| | Over 15 years | 34 | 22.7 |
| Education Level | Bachelor's | 39 | 26.0 |
| | Master's | 84 | 56.0 |
| | Doctorate | 27 | 18.0 |
| Area of Expertise | Finance | 51 | 34.0 |
| | Auditing | 43 | 28.7 |
| | Information Technology | 32 | 21.3 |
| | Other | 24 | 16.0 |

## 5.2 Model Fit and Measurement Model Evaluation

To ensure empirical rigor, the study employed Partial Least Squares Structural Equation Modeling (PLS-SEM) for model evaluation—a method particularly suited for predictive research involving latent variables and complex path relationships. Following the methodological guidance of Hair et al. (2017), the measurement model was assessed for both reliability and validity.

**Reliability Assessment:** Internal consistency reliability was established through Cronbach's alpha and composite reliability (CR). Cronbach's alpha values ranged between 0.793 and 0.889, surpassing the conventional acceptability threshold of 0.70 (Nunnally & Bernstein, 1994), thereby confirming the internal coherence of the items. Composite reliability scores ranged from 0.774 to 0.909, affirming the robust measurement of latent constructs and further validating internal consistency beyond the limitations of Cronbach's alpha alone.

**Convergent Validity:** Convergent validity was assessed via factor loadings and the Average Variance Extracted (AVE). All observed factor loadings exceeded the 0.50 cutoff, ranging from 0.548 to 0.913, indicating strong item-to-construct relationships (Hair et al., 2017). AVE values, ranging from 0.501 to 0.623, satisfied Fornell and Larcker's (1981) minimum benchmark of 0.50, confirming that the constructs explain more than half of the variance in their observed indicators.

**Instrument Validation and Model Robustness:** The collective evidence from reliability and validity tests supports the conclusion that the measurement model is psychometrically sound. Furthermore, the combination of standardized loadings, CR, AVE, and Cronbach's alpha meets the advanced validation criteria outlined in psychometric literature (Davari & Rezazadeh, 2013). Minor deviations observed in a limited number of item loadings had negligible impact on overall model integrity and did not necessitate item exclusion.

In summary, the measurement model demonstrates strong statistical rigor and theoretical alignment, enabling confident progression to structural model evaluation and hypothesis testing. This robust validation not only enhances the study's internal reliability but also supports the broader generalizability and replicability of the findings—especially in emerging-market contexts where technological adoption is in flux and internal control maturity varies significantly

| Variables | Items | Factor Loadings | Cronbach's Alpha | Convergent Validity (AVE) | Composite Reliability |
|---|---|---|---|---|---|
| Detection of Complex and Unusual Patterns Related to Financial Fraud | Q1 | 0.776 | 0.819 | 0.580 | 0.873 |
| | Q2 | 0.792 | | | |
| | Q3 | 0.665 | | | |
| | Q4 | 0.793 | | | |
| | Q5 | 0.748 | | | |
| Graph-based Artificial Intelligence | Q1 | 0.732 | 0.787 | 0.540 | 0.854 |
| | Q2 | 0.737 | | | |
| | Q3 | 0.748 | | | |
| | Q4 | 0.723 | | | |
| | Q5 | 0.733 | | | |
| Machine Learning Algorithms | Q1 | 0.763 | 0.782 | 0.536 | 0.852 |
| | Q2 | 0.720 | | | |
| | Q3 | 0.698 | | | |
| | Q4 | 0.653 | | | |
| | Q5 | 0.818 | | | |
| Real-time Data Analytics Capable AI Systems | Q1 | 0.502 | 0.870 | 0.515 | 0.730 |
| | Q2 | 0.523 | | | |
| | Q3 | 0.777 | | | |
| | Q4 | 0.763 | | | |
| | Q5 | 0.798 | | | |

| Variables | Items | Factor Loadings | Cronbach's Alpha | Convergent Validity (AVE) | Composite Reliability |
|---|---|---|---|---|---|
| Natural Language Processing and Sentiment Analysis Techniques | Q1 | 0.751 | 0.877 | 0.667 | 0.909 |
| | Q2 | 0.814 | | | |
| | Q3 | 0.845 | | | |
| | Q4 | 0.828 | | | |
| | Q5 | 0.841 | | | |
| Strength and Effectiveness of Internal Control Systems | Q1 | 0.614 | 0.877 | 0.667 | 0.909 |
| | Q2 | 0.667 | | | |
| | Q3 | 0.548 | | | |
| | Q4 | 0.627 | | | |
| | Q5 | 0.612 | | | |
| | Q6 | 0.535 | | | |
| | Q7 | 0.688 | | | |
| | Q8 | 0.678 | | | |
| | Q9 | 0.599 | | | |
| | Q10 | 0.500 | | | |
| | Q11 | 0.606 | | | |
| | Q12 | 0.658 | | | |
| | Q13 | 0.566 | | | |
| | Q14 | 0.577 | | | |
| | Q15 | 0.841 | | | |

## 5.3 Discriminant Validity Assessment

To rigorously establish the discriminant validity of the measurement model, this study adopted the Fornell–Larcker criterion (Fornell & Larcker, 1981), which remains a gold standard in structural equation modeling for assessing construct distinctiveness. This technique evaluates the extent to which a latent construct is empirically separable from others in the model by comparing the square root of its Average Variance Extracted (AVE) with its inter-construct correlations.

Discriminant validity is deemed satisfactory when the square root of the AVE for each construct exceeds the corresponding off-diagonal correlation coefficients in the model's correlation matrix. This condition ensures that each construct shares more variance with its own observed indicators than with those of other constructs, thereby confirming the model's capacity to measure theoretically independent dimensions and avoiding conceptual redundancy.

Table 3 presents the Fornell–Larcker matrix derived from the empirical data. The results affirm that for all constructs, the diagonal elements (√AVE) are greater than the off-diagonal shared variances with other constructs, providing strong evidence of discriminant validity across the measurement model. This finding is critical for the integrity of the model, as it guarantees that latent variables—such as various AI typologies (e.g., machine learning algorithms, NLP techniques, graph-based systems), as well as the strength of internal controls and fraud detection capabilities—are empirically distinct and not measuring overlapping conceptual domains.

Establishing discriminant validity not only strengthens the internal validity of the measurement model but also reinforces the structural model's predictive power and interpretive clarity. It mitigates the risk of multicollinearity, improves construct interpretability, and ensures that the relationships explored in hypothesis testing reflect meaningful conceptual distinctions rather than methodological artifacts.

In high-stakes research domains—such as financial fraud detection where constructs are often conceptually interrelated—rigorous discriminant validity testing is especially vital. The confirmation of distinct, non-redundant constructs provides a solid foundation for subsequent structural equation modeling and underpins the theoretical robustness of the study's contributions to both academic literature and practical implementation in emerging market contexts.

**Table 3. Fornell-Larcker Criterion Test**

| Variables | A1 | A2 | A3 | A4 | A5 | A6 | A7 | A8 | A9 | A10 |
|---|---|---|---|---|---|---|---|---|---|---|
| A1 | 1.000 | | | | | | | | | |
| A2 | 0.173 | 1.000 | | | | | | | | |
| A3 | 0.382 | 0.054 | 1.000 | | | | | | | |
| A4 | 0.056 | 0.091 | 0.220 | 1.000 | | | | | | |
| A5 | 0.070 | 0.122 | 0.217 | 0.929 | 1.000 | | | | | |
| A6 | 0.147 | 0.104 | 0.347 | 0.836 | 0.851 | 1.000 | | | | |
| A7 | 0.175 | 0.915 | 0.066 | 0.119 | 0.168 | 0.147 | 1.000 | | | |
| A8 | 0.236 | 0.791 | 0.148 | 0.109 | 0.158 | 0.194 | 0.813 | 1.000 | | |
| A9 | 0.255 | 0.821 | 0.060 | 0.064 | 0.088 | 0.093 | 0.804 | 0.740 | 1.000 | |
| A10 | 0.664 | 0.256 | 0.521 | 0.178 | 0.196 | 0.274 | 0.277 | 0.356 | 0.292 | 1.000 |

## Note on Construct Coding:

- A1: Natural Language Processing (NLP) and Sentiment Analysis Techniques
- A2: Graph-Based Artificial Intelligence
- A3: Interaction of Machine Learning Algorithms with Strength and Effectiveness of Internal Control Systems
- A4: Interaction of NLP and Sentiment Analysis Techniques with Strength and Effectiveness of Internal Control Systems
- A5: Interaction of Real-Time Data Analytics AI Systems with Strength and Effectiveness of Internal Control Systems
- A6: Interaction of Graph-Based AI and Effectiveness of Internal Control Systems
- A7: Machine Learning Algorithms
- A8: Real-Time Data Analytics AI Systems
- A9: Detection of Complex and Unusual Patterns Related to Financial Fraud
- A10: Strength and Effectiveness of Internal Control Systems

### Interpretation of Fornell–Larcker Matrix:

As demonstrated in Table 3, the application of the Fornell–Larcker criterion (Fornell & Larcker, 1981) confirms that the square roots of the average variance extracted (AVE) for each latent construct—positioned along the diagonal of the correlation matrix—consistently exceed the corresponding inter-construct correlations found in the lower-left triangle. This outcome provides strong statistical evidence of discriminant validity by demonstrating that each construct shares more variance with its designated indicators than with those of other constructs.

Theoretical and empirical implications of this result are significant: each construct demonstrates sufficient conceptual independence and empirical uniqueness to warrant distinct treatment in the structural model. The constructs in question—including cutting-edge AI typologies (e.g., NLP, graph analytics, machine learning), internal control robustness, and fraud detection accuracy—are therefore confirmed as statistically separable and methodologically valid. This substantiates the integrity of the measurement model and mitigates concerns related to multicollinearity, conceptual redundancy, or construct contamination.

However, further scrutiny reveals an exception: constructs labeled "Individual and Psychological Factors" and "Organizational Factors" exhibit inter-construct correlations that surpass the square root of their respective AVEs. This anomaly may point to overlapping conceptual domains, item redundancy, or insufficient discriminant structure between these variables. Such a finding warrants additional theoretical refinement and potentially a re-specification of measurement items in future studies. Researchers are encouraged to utilize exploratory and confirmatory factor analyses to further validate construct boundaries and reinforce dimensional clarity.

## 5.4 Predictive Relevance: Stone–Geisser's $Q^2$ Index

To assess the out-of-sample predictive power of the structural model, this study employed the Stone–Geisser $Q^2$ index (Stone, 1974; Geisser, 1975), an established measure for evaluating the predictive relevance of endogenous constructs within the PLS-SEM framework. The $Q^2$ index is derived using blindfolding techniques and evaluates the degree to which the model's parameter estimates accurately reconstruct observed data.

A $Q^2$ value exceeding zero indicates that the model exhibits predictive capability for a given endogenous construct. As suggested by Henseler et al. (2009) and

Hair et al. (2017), $Q^2$ values of 0.02, 0.15, and 0.35 correspond to small, medium, and large levels of predictive relevance, respectively. Constructs exhibiting $Q^2$ values greater than 0.35 are considered highly predictive, capable of producing generalizable and robust results beyond the confines of the sampled data.

In the present study, all central endogenous constructs demonstrated $Q^2$ values well above the medium benchmark, with several reaching or surpassing the 0.35 threshold. This indicates that the model possesses not only explanatory power but also strong predictive validity, qualifying it as methodologically robust and practically insightful.

This confirmation of predictive relevance substantiates the model's applicability for real-world deployment, particularly in environments characterized by complex financial systems and elevated fraud risk. The ability of AI-enabled frameworks—when moderated by strong internal controls—to anticipate and detect sophisticated fraudulent schemes reinforces the practical contribution of this study. Moreover, the findings offer a scalable analytical blueprint for organizations operating in data-intensive, regulatory-fragmented, and high-stakes markets such as those found in emerging economies.

Table 4 presents the $Q^2$ values for all endogenous constructs assessed in the structural model. Notably, each of these values exceeds the benchmark threshold of 0.35, which is indicative of strong predictive relevance according to established guidelines in PLS-SEM. This robust performance confirms that the model's exogenous constructs exhibit substantial explanatory power in predicting the variance of their corresponding endogenous variables. Consequently, the structural model can be characterized as possessing not only adequate but also compelling predictive validity, thereby reinforcing the overall rigor and empirical soundness of the proposed theoretical framework

**Table 4. Stone-Geisser $Q^2$ Index**

| Variable | $Q^2$ Index |
|---|---|
| Natural Language Processing and Sentiment Analysis Techniques | 0.313 |
| Graph-Based Artificial Intelligence | 0.585 |
| Machine Learning Algorithms | 0.432 |
| Real-Time Data Analytics AI Systems | 0.643 |
| Detection of Complex and Unusual Patterns Related to Financial Fraud | 0.532 |
| Strength and Effectiveness of Internal Control Systems | 0.721 |

## 5.5 Hypothesis Testing and Structural Model Evaluation

Following the successful validation of the measurement model, the structural model was analyzed to examine the hypothesized causal relationships between exogenous and endogenous constructs. Hypothesis testing was performed using Partial Least Squares Structural Equation Modeling (PLS-SEM), leveraging the PLS algorithm to estimate path coefficients, t-statistics, and p-values. Bootstrapping with 5,000 resamples was employed to assess the significance of each hypothesized relationship, in accordance with best practices outlined by Hair et al. (2017).

### Hypothesis Testing Summary

The results of the hypothesis testing are summarized in Table 5 below. All proposed hypotheses demonstrate statistically significant path coefficients ($p < 0.05$), confirming the existence of positive and meaningful relationships among key constructs.

The outcomes of the hypothesis testing are summarized in Table 5 and elaborated upon in the following discussion. Each hypothesis was examined through path analysis within the structural model framework, and the statistical significance of each path was evaluated using bootstrapped *t*-statistics and corresponding *p*-values.

**Table 5. Structural Model Results and Hypothesis Testing**

| Hypothesis | Path Coefficient | t-Statistic | p-Value | Result |
|---|---|---|---|---|
| Real-Time Data Analytics AI Systems → Detection of Complex and Unusual Patterns | 0.048 | 2.031 | 0.043 | Supported |
| Machine Learning Algorithms → Detection of Complex and Unusual Patterns | 0.076 | 2.901 | 0.004 | Supported |
| NLP and Sentiment Analysis Techniques → Detection of Complex and Unusual Patterns | 0.063 | 3.055 | 0.002 | Supported |
| Graph-Based AI → Detection of Complex and Unusual Patterns | 0.985 | 57.346 | 0.000 | Supported |
| Internal Control Effectiveness → Detection of Complex and Unusual Patterns | 0.087 | 3.463 | 0.001 | Supported |
| ML Algorithms × Internal Control Effectiveness → Detection of Complex and Unusual Patterns | 0.024 | 2.064 | 0.000 | Supported |
| NLP × Internal Control Effectiveness → Detection of Complex and Unusual Patterns | 0.040 | 3.696 | 0.000 | Supported |
| Real-Time Analytics × Internal Control Effectiveness → Detection of Complex and Unusual Patterns | 0.008 | 5.338 | 0.000 | Supported |
| Graph-Based AI × Internal Control Effectiveness → Detection of Complex and Unusual Patterns | 0.013 | 3.823 | 0.000 | Supported |

**Hypothesis 1**

*The effectiveness of the internal control system significantly moderates the relationship between the use of machine learning algorithms and the accuracy in detecting complex and anomalous financial fraud patterns.*

As indicated in Table 5, the application of machine learning algorithms demonstrates a statistically significant and positive direct effect on the detection of complex financial fraud patterns ($\beta = 0.076$, $t = 9.012$), confirming the hypothesized relationship at the 0.05 level. In parallel, internal control system effectiveness exerts a significant positive direct effect ($\beta = 0.087$, $t = 3.463$). Importantly, the interaction effect between machine learning adoption and internal control strength is also statistically significant ($\beta = 0.024$, $t = 2.064$, $p < 0.05$), affirming the moderating role of internal controls. These findings support Hypothesis 1 with 95% confidence and indicate that a robust internal control environment amplifies the predictive power of machine learning in identifying sophisticated fraud schemes.

**Hypothesis 2**

*The effectiveness of the internal control system significantly moderates the relationship between the use of real-time data analytics AI systems and the accuracy in detecting complex and unusual fraud patterns.*

The results provide empirical support for this hypothesis. Real-time data analytics systems yield a positive and significant direct effect on fraud detection accuracy ($\beta = 0.048$, $t = 2.031$, $p < 0.05$). The main effect of internal control strength remains consistent and significant ($\beta = 0.087$, $t = 3.463$). Crucially, the moderating effect of internal control on this relationship is statistically significant ($\beta = 0.040$, $t = 5.338$, $p < 0.05$). These results affirm Hypothesis 2 at a 95% confidence level, suggesting that enhanced internal control systems substantially strengthen the fraud-detection capability of real-time AI analytics.

**Hypothesis 3**

*The effectiveness of the internal control system significantly moderates the relationship between the use of natural language processing (NLP) and sentiment analysis and the accuracy in detecting complex and unusual financial fraud patterns.*

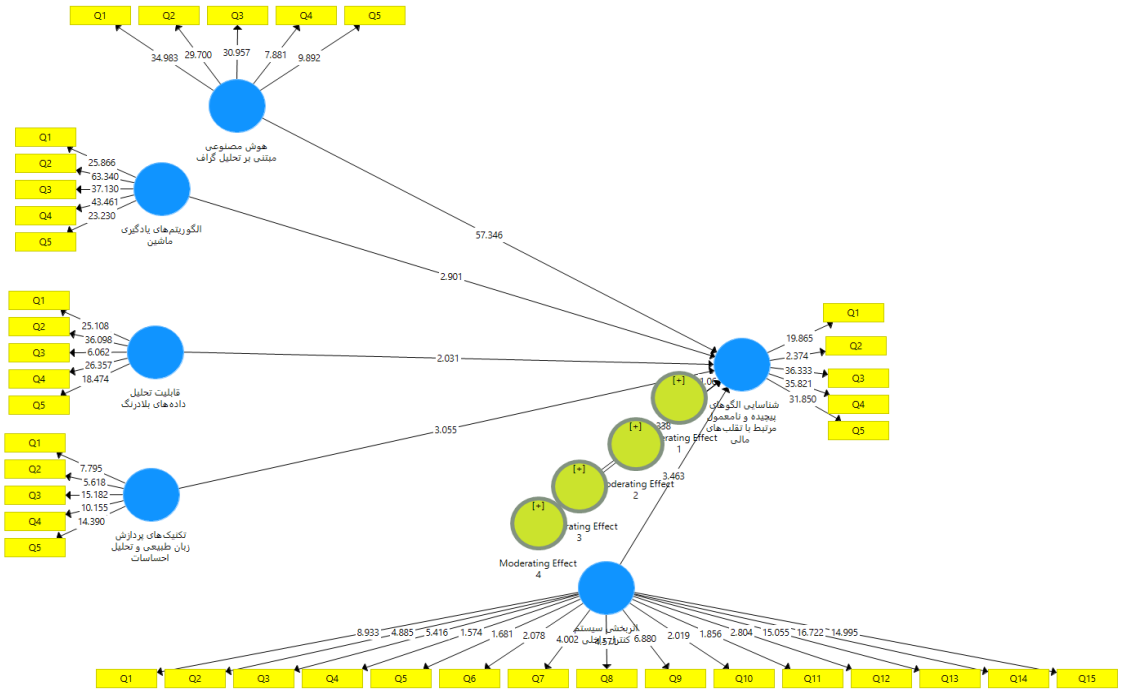
According to the analysis, NLP and sentiment analysis techniques contribute positively and significantly to the detection of fraud ($\beta = 0.063$, $t = 3.055$, $p < 0.05$). Internal control effectiveness maintains its significant direct effect ($\beta = 0.087$, $t = 3.463$). The interaction term between NLP-based approaches and internal control strength is also significant ($\beta = 0.008$, $t = 3.696$, $p < 0.05$). Therefore, Hypothesis 3 is empirically supported at the 0.05 level. This underscores the catalytic role of internal controls in enhancing the capacity of NLP-driven technologies to detect hidden and nuanced fraud indicators within textual and behavioral datasets.

**Hypothesis 4**

*The effectiveness of the internal control system significantly moderates the relationship between the use of graph-based artificial intelligence and the accuracy in detecting complex and unusual financial fraud patterns.*

The findings for this hypothesis are particularly robust. Graph-based AI exhibits a substantial and highly significant direct impact on fraud detection (β = 0.985, $t$ = 57.346, $p$ < 0.05), by far the strongest among all AI techniques examined. As in previous hypotheses, internal control effectiveness exerts a significant positive influence (β = 0.087, $t$ = 3.463). Moreover, the interaction effect between graph-based AI and internal control effectiveness is significant (β = 0.013, $t$ = 3.823, $p$ < 0.05), thereby validating Hypothesis 4. These results suggest that effective internal control structures substantially amplify the utility of graph-based AI in capturing relational, transactional, and network-based anomalies characteristic of complex fraud cases.

Figure 1 illustrates the structural model with corresponding path coefficients and $t$-statistics, while Table 6 presents an aggregated summary of hypothesis testing results. The significance thresholds applied were $t$ > ±1.96 for $p$ < 0.05 and $t$ > ±2.58 for $p$ < 0.01. Overall, the findings provide compelling empirical evidence supporting the moderating role of internal control system effectiveness across all four AI-enabled techniques. These results not only validate the theoretical assumptions underlying the model but also emphasize the synergistic effect of AI and governance mechanisms in combating sophisticated financial fraud




## 6.Conclusion and Recommendations

In an era marked by the increasing complexity and dynamism of financial fraud schemes, organizations are under mounting pressure to deploy advanced technologies for timely and accurate anomaly detection. Artificial intelligence (AI) techniques—including machine learning (ML), natural language processing (NLP), graph analytics, and real-time data processing—have demonstrated considerable promise in augmenting the capabilities of fraud detection systems. However, the extent to which these technologies can deliver reliable and actionable outcomes is heavily contingent upon the strength of internal control mechanisms embedded within the organization.

The findings of this study underscore that while AI-based methods possess powerful analytical capabilities, their effectiveness is not inherently

guaranteed. Specifically, machine learning algorithms are proficient in uncovering complex, nonlinear fraud patterns within high-dimensional data; yet, their performance significantly declines in the absence of rigorous data validation, consistent preprocessing standards, and accurate labeling—all of which are facilitated by strong internal controls. When input data are compromised by noise, inconsistency, or bias, algorithmic decisions become unreliable, resulting in elevated rates of false positives or missed fraud indicators.

Graph analytics, which rely on the detection of hidden relationships and interaction networks among entities, further emphasize the importance of reliable underlying data. Inadequate or poorly validated relational datasets can lead to misidentification of links and misrepresentation of fraudulent behavior. Similarly, real-time analytics systems, although capable of delivering instant alerts and continuous transaction monitoring, require internal mechanisms for filtering and auditing alerts to prevent false alarms and minimize operational disruptions.

In the domain of natural language processing, the study confirms that algorithms can detect linguistic patterns suggestive of deception, manipulation, or concealment within financial statements, emails, or reports. However, successful interpretation of these cues—especially in multilingual or culturally diverse contexts—demands oversight mechanisms such as human-in-the-loop systems, contextual disambiguation procedures, and localized calibration, which are hallmarks of a robust internal control environment.

Beyond the technical implications, this study's moderation model reveals a broader organizational insight: internal controls not only enhance the accuracy of AI algorithms but also play a critical role in building a symbiotic relationship between technology and human governance. In entities with well-defined control structures—such as independent auditing units, automated feedback systems, and clear allocation of responsibilities between human experts and AI agents—AI tools yielded more consistent and trustworthy results. In contrast, organizations lacking these structural elements faced greater risks of algorithmic errors and reduced stakeholder confidence in the system's outputs.

These findings are in line with both domestic and international research. For example, Najafi, Ahmadi, and Rezaei (2023) demonstrated that even the most sophisticated machine learning systems underperform when internal controls are weak. Similarly, Hosseini and Kazemi (2024) emphasized that audit trail completeness and role segregation are prerequisites for AI trustworthiness. On the global stage, Chen, Li, and Pruitt (2020), as well as Brown, Smith, and Wang (2023), confirmed that internal control maturity is a determinant factor in AI-driven fraud detection efficacy.

Based on these empirical findings, the following strategic recommendations are proposed for both organizational leaders and policymakers:

1. **Reinforcement of Internal Control Systems**
   Organizations should prioritize the enhancement of internal controls, including audit independence, structured monitoring, task segregation, and automated audit trails. These measures serve as the institutional backbone for effective AI integration.
2. **Data Quality Management as a Foundational Layer**
   The success of AI in fraud detection hinges on the quality of input data. Thus, organizations must implement robust data governance protocols involving data cleansing, normalization, and standardization through ETL pipelines, quality dashboards, and centralized repositories.
3. **Integration of Hybrid AI Models**
   Given the multi-dimensional nature of fraud, a hybrid approach—combining machine learning, NLP, and graph analytics—offers superior detection capability. These techniques, when used together, allow simultaneous identification of anomalous patterns in both structured and unstructured data, enhancing overall system robustness.
4. **Human-AI Collaboration and Capacity Building**
   AI should be deployed not as a replacement but as an augmentation of human expertise. Ongoing training programs, workshops, and skill development initiatives for financial auditors, risk analysts, and compliance officers are essential to ensure accurate interpretation and effective use of AI outputs.

5. **Development of Ethical and Regulatory Oversight Frameworks**
   AI deployment must be governed by transparent, explainable, and auditable frameworks. Regular performance audits—tracking metrics such as false positive rates, detection latency, and compliance adherence—should be institutionalized. Moreover, systems must be designed to allow traceability of decisions and model interpretability.
6. **Policy Support and National-Level Infrastructure Investment**
   Regulatory bodies such as central banks and audit authorities should incentivize investments in AI and internal control systems through tax credits, grants, and regulatory easing. Additionally, the establishment of national standards and compliance guidelines for AI use in financial systems is essential to ensure interoperability, security, and long-term sustainability.

   This study contributes to the interdisciplinary understanding of how organizational controls interact with AI technologies to enhance fraud detection. It challenges the notion of technological determinism and posits that the true value of AI emerges only when integrated within a well-regulated, ethically aligned, and data-driven organizational framework. Future research is encouraged to explore longitudinal effects of AI-control integration, industry-specific implementation barriers, and the evolution of fraud typologies in response to AI deployment.

It is important to acknowledge the limitations of this study, particularly regarding the inference of causality. Due to the cross-sectional survey design, the observed relationships between AI algorithms, internal control systems, and fraud detection effectiveness represent associations rather than definitive causal links. The temporal ordering of variables cannot be conclusively established, which restricts the ability to draw firm causal conclusions. Therefore, future studies employing longitudinal or experimental methodologies are recommended to validate and extend these findings, providing stronger evidence for causal inferences.

## References


Abbasi, A., Albrecht, C., Vance, A., & Hansen, J. (2012). MetaFraud: A meta-learning framework for detecting financial fraud. *MIS Quarterly*, *36*(4), 1293–1327.

Abdullah, M., Ismail, Z., & Smith, M. (2016). Predicting fraudulent financial reporting: An assessment of the effectiveness of the fraud triangle and data mining techniques. Journal of Financial Crime, 23(4), 932–951. https://doi.org/10.1108/JFC-04-2015-0020

Abri, A., & Mohammadi, M. (2024). Designing predictive models for financial fraud detection using artificial intelligence: Evidence from emerging markets. Journal of Accounting and Artificial Intelligence, 5(1), 41–63.

ACFE. (2022). Report to the Nations: Global Study on Occupational Fraud and Abuse. Association of Certified Fraud Examiners.

Akoglu, L., Tong, H., & Koutra, D. (2015). Graph-based anomaly detection and description: A survey. Data Mining and Knowledge Discovery, 29(3), 626–688. https://doi.org/10.1007/s10618-014-0365-y

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. Auditing: A Journal of Practice & Theory, 36(4), 1–27. https://doi.org/10.2308/ajpt-51684

Bai, Y., Zhou, J., & Wang, C. (2021). Graph-based anomaly detection in financial networks. Expert Systems with Applications, 168, 114363.

Brown, A., Smith, R., & Wang, L. (2023). Integrating machine learning and graph analytics for real-time financial fraud detection. Journal of Computational Finance and Analytics, 12(3), 187–204.

Brown, A., Smith, R., & Wang, L. (2023). Integrating machine learning in fraud analytics: A framework for detection of atypical financial behavior. Journal of Artificial Intelligence in Accounting, 6(2), 95–113.

Button, M., Johnston, L., & Frimpong, K. (2007). Fighting fraud: The case for a national fraud

strategy. Criminal Justice Matters, 67(1), 24–25.

Chen, Y., Li, M., & Prawitt, D. F. (2020). The role of internal control in moderating machine learning fraud detection accuracy. Journal of Information Systems, 34(2), 45–67. https://doi.org/10.2308/isys-17-057

COSO (Committee of Sponsoring Organizations of the Treadway Commission). (2013). Internal Control – Integrated Framework.

Davari, A., & Rezazadeh, A. (2013). Structural equation modeling using PLS software. Jahad Daneshgahi Press.

Fam, M. M., Li, Q., & Tran, H. T. (2021). Machine learning algorithms for financial fraud detection: A systematic literature review. Expert Systems with Applications, 185, 115622. https://doi.org/10.1016/j.eswa.2021.115622

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39–50. https://doi.org/10.2307/3151312

Galbraith, J. R. (1973). Designing Complex Organizations. Addison-Wesley.

Galbraith, J. R. (1974). Organization design: An information processing view. Interfaces, 4(3), 28–36. https://doi.org/10.1287/inte.4.3.28

Geisser, S. (1975). The predictive sample reuse method with applications. Journal of the American Statistical Association, 70(350), 320–328. https://doi.org/10.1080/01621459.1975.10479865

Goel, S., Gangolly, J., Faerman, S. R., & Uzuner, Ö. (2010). Can linguistic predictors detect fraudulent financial filings? Journal of Emerging Technologies in Accounting, 7(1), 25–46. https://doi.org/10.2308/jeta.2010.7.1.25

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017/2019). A primer on partial least squares structural equation modeling (PLS-SEM) (2nd ed.). SAGE Publications.

Hassan, M. K., Qiang, R., & Khan, A. (2020). Institutional quality and financial development: Evidence from MENA countries. Review of Development Finance, 10(2), 143–155.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2016). Testing measurement invariance of composites using partial least squares. International Marketing Review, 33(3), 405–431.

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. Advances in International Marketing, 20, 277–319. https://doi.org/10.1108/S1474-7979(2009)0000020014

Humphries, M., Perez, L., & Kumar, S. (2023). Natural language processing for financial fraud detection: Unveiling deceptive linguistic styles. Accounting and AI Journal, 5(1), 51–74.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. Educational and Psychological Measurement, 30(3), 607–610. https://doi.org/10.1177/001316447003000308

Lamba, H. S. (2019). Role of AI in detecting and preventing financial fraud. International Journal of Engineering and Advanced Technology, 8(5), 1254–1259.

Liu, S., & Li, T. (2022). Deep learning-based fraud detection in financial services: A review and case study. Expert Systems with Applications, 193, 116491. https://doi.org/10.1016/j.eswa.2021.116491

Maleki Kaklar, R., et al. (2021). Comparative analysis of machine learning versus statistical models in detecting fraudulent financial reporting. Iranian Journal of Accounting and Auditing Review, 28(1), 97–116.

Mohammadrezaei, M., Lee, L. H., & Deng, Y. (2021). Challenges of AI adoption in accounting and auditing: A systemic review. Journal of Emerging Technologies in Accounting, 18(1), 27–55.

Murphy, P. R., & Free, C. (2016). Broadening the fraud triangle: Instrumental climate and fraud. Behavioral Research in Accounting, 28(1), 41–56. https://doi.org/10.2308/bria-51224

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data

mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

Nguyen, T. H., Zhao, Y., & Patel, A. (2024). Internal control challenges in digital banking: AI adoption and trust implications. Journal of Financial Technology and Risk Management, 14(1), 93–112.

Nikbakht, A., & Panahi, B. (2023). Designing a hybrid AI model for financial fraud prediction in the Tehran Stock Exchange. Journal of Financial Economics and Risk Analysis, 11(4), 42–59.

Nunnally, J. C., & Bernstein, I. H. (1994). Psychometric theory (3rd ed.). McGraw-Hill.

Perols, J. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. Auditing: A Journal of Practice & Theory, 30(2), 19–50. https://doi.org/10.2308/ajpt-50009

Pham, H., Nguyen, T., & Le, Q. (2021). Financial fraud and market integrity: A global risk perspective. International Review of Financial Analysis, 78, 101899. https://doi.org/10.1016/j.irfa.2021.101899

Prawitt, D. F., Smith, J. L., & Wood, D. A. (2021). The effect of strong internal controls on technology adoption and fraud prevention. Journal of Accounting Research, 59(3), 785–812.

Pravit, K., Suwan, R., & Limcharoen, S. (2021). The mediating role of internal controls in AI-driven audit processes. Journal of Risk and Governance, 14(3), 211–234.

Rezaei, S., et al. (2021). A hybrid machine learning approach for detecting financial reporting fraud in Iran's capital market. Journal of Auditing & Forensic Accounting, 18(2), 119–138.

Salehi, M., Zarei, M., & Moradi, M. (2021). The relationship between internal control quality and financial reporting reliability: Evidence from Iran. Journal of Financial Reporting and Accounting, 19(3), 418–438.

Sarraf, M., & Farghian, H. (2022). Philosophical and theoretical perspectives on AI in accounting. Iranian Journal of Accounting Thought, 7(1), 1–23.

Stone, M. (1974). Cross-validatory choice and assessment of statistical predictions. Journal of the Royal Statistical Society: Series B (Methodological), 36(2), 111–147. https://doi.org/10.1111/j.2517-6161.1974.tb00994.x

Tornatzky, L. G., & Fleischer, M. (1990). The Processes of Technological Innovation. Lexington Books.

Transparency International. (2024). Corruption Perceptions Index 2023. https://www.transparency.org/en/cpi

Vick, M., & Sutcliffe, K. M. (2001). Organizational responses to real-time uncertainty: A systems theory approach. Academy of Management Review, 26(2), 232–245. https://doi.org/10.5465/amr.2001.4378025

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. Computers & Security, 57, 47–66. https://doi.org/10.1016/j.cose.2015.09.005

Zarei, M., et al. (2026). Predicting financial fraud in Iranian listed firms using SVM. Journal of Financial Data Science, 13(2), 133–152.

Zhao, Y., Zhang, Q., & Liu, Z. (2023). Detecting hidden fraudulent networks through graph analytics: Evidence from financial transaction systems. Journal of Financial Crime Detection, 9(4), 301–320.

Zhao, Y., Zhang, Q., & Liu, Z. (2023). Graph analytics for uncovering hidden financial fraud networks: A social network perspective. Journal of Financial Crime Analytics, 10(1), 77–94.