Knowledge Processing Studies. 2025, 17, 5(4): 62-77.

International Journal of Knowledge Processing Studies
(KPS)

Homepage: http://kps.artahub.ir/

ORIGINAL RESEARCH ARTICLE

Designing a Knowledge Model for Accounting Fraud Detection Based on Digital Innovations with a Focus on Human-Technology Interaction in Organizations

Reza Nemati Mofarrah[1], Farzin Rezaei[2,*], Hosein Kazemi[3], Kumars Biglar[4]

[1]*PhD Candidate, Department of Accounting, Qa .c., Islamic Azad University , Qazvin, Iran.* reza.nematimofarrah@iau.ac.ir

[2]*Professor, Department of Accounting, Qa .c., Islamic Azad University , Qazvin , Iran. (Corresponding author)* farzin.rezaei@iau.ac.ir, *0009-0005-7987-7650.*

[3]*Assistant Professor, Department of Accounting, Qa .c., Islamic Azad University, Qazvin, Iran.* hosein.kazemi@iau.ac.ir

[4]*Assistant Professor, Department of Accounting, Qa .c., Islamic Azad University, Qazvin, Iran.* kumars.biglar@iau.ac.ir

ARTICLE INFO

Article History:
Received: 2025-09-21
Revised: 2025-10-01
Accepted: 2025-11-27
Published Online: 2025-12-01

Keywords:
Fraud detection knowledge model, Accounting fraud detection, Digital innovations, Human-technology interaction.

Number of Reference: 40
Number of Figures: 8
Number of Tables: 8

DOI:
10.22034/kps.2026.567819.1263

ABSTRACT

The aim of the research is to design a knowledge model for accounting fraud detection based on digital innovations with a focus on human-technology interaction in organizations. The increasing spread of digital innovations and the increasing complexity of financial processes have fundamentally changed the nature of accounting fraud in organizations and challenged the effectiveness of traditional fraud detection approaches. In such circumstances, relying solely on technological tools or human judgments alone is not sufficient to detect fraud in a timely and effective manner, but the synergy of human knowledge and the capacities of digital technologies has become doubly important. The structural interaction analysis method of MICMAC software was used in information processing. Based on the results obtained, 10 criteria (big data analytics, fraud machine learning, audit artificial intelligence, smart transaction tracking, encryption and transparency, financial process automation, hidden behavioral data mining, digital anomaly detection, financial blockchain platform, and continuous real-time monitoring) were categorized into 7 levels. This approach, by creating synergy between the professional knowledge of accountants and auditors, the analytical capabilities of smart technologies, and organizational knowledge sharing and learning platforms, enables more timely and accurate identification of fraud patterns. The results of such a model can lead to improved financial transparency, strengthened stakeholder trust, improved supervisory decision-making, and organizations moving toward predictive and knowledge-based control systems; which will ultimately play an important role in improving the economic health and financial governance of organizations. **©authors**.

►**Citation:** Nemati Mofarrah, R., Rezaei, F., Kazemi, H., & Biglar, K. (2025). Designing a Knowledge Model for Accounting Fraud Detection Based on Digital Innovations with a Focus on Human-Technology Interaction in Organizations. *International Journal of Knowledge Processing Studies (KPS)*, 5(4): 62-77. Doi: 10.22034/kps.2026.567819.1263

1. Introduction

In recent decades, the phenomenon of accounting fraud has been considered one of the most serious challenges to economic and organizational systems, especially in developing countries, including Iran (Khademi, 2024). Accounting fraud not only causes deviations in financial reporting and economic decision-making, but also weakens the trust of stakeholders, investors, regulatory institutions, and the general public in the health of the financial system (Gkegkas et al., 2025). In the Iranian economy, which is faced with features such as the prominent role of the government, the complexity of organizational structures, international sanctions, restrictions on information transparency, and environmental pressures on organizations, the ground for more complex and sometimes more hidden accounting fraud has been prepared. These conditions make the need to rethink traditional approaches to fraud detection and move towards new, intelligent, and knowledge-based models more apparent than ever (Bhattacharya, 2024).

Traditional approaches to detecting accounting fraud in Iran have been mainly based on retrospective inspections, manual controls, individual judgments of auditors, and limited use of analytical tools (Bagherian Kasgari et al., 2024). Although these approaches have been effective at times, they face serious limitations in the face of the increasing complexity of financial operations, the massive volume of data, the high speed of transactions, and the diversity of new fraud methods (Alsulami, 2023). On the other hand, focusing solely on formal rules and controls, without considering the knowledge, behavioral, and technological contexts of organizations, has resulted in many frauds either not being detected or being detected at very late stages. This issue has had widespread economic and social consequences in Iranian organizations, especially large companies, banks, insurance companies, and public institutions (Hernández-Aros, 2024).

At the same time, new developments in digital technologies have provided unprecedented opportunities to redesign fraud detection systems. Technologies such as artificial intelligence, machine learning, big data analytics, blockchain, intelligent accounting systems, process automation, and predictive analytics tools enable the identification of hidden patterns, abnormal behaviors, and complex financial relationships with high accuracy and speed (Compagnin, 2025). However, the experience of organizations shows that the mere deployment of digital technologies, without considering human knowledge, organizational interactions, and the culture of using technology, does not necessarily lead to effective fraud detection. In many cases, the gap between humans and technology, the lack of acceptance of intelligent systems, the weakness in interpreting technological outputs, and the lack of organizational learning have reduced the effectiveness of these tools (Mijani et al., 2025).

In the meantime, the concept of “knowledge model of accounting fraud detection” is proposed as a new approach that emphasizes the integration of human knowledge, technological knowledge, and organizational knowledge. Beyond a technical system or a set of controls, the knowledge model seeks to design a framework in which fraud-related knowledge is produced, shared, applied, and updated in a systematic and dynamic manner (Oladejo et al., 2020). In such a model, auditors, financial managers, employees, intelligent systems, and regulatory institutions all play a role as knowledge actors in the fraud detection process. This approach is particularly important in the Iranian context, where human knowledge capital plays an important role in compensating for structural limitations (Shevchu, 2025). One of the neglected dimensions in existing research and practices in Iran is the focus on human-technology interaction in the accounting fraud detection process. Human-technology interaction refers to the way human users and digital systems communicate, trust, interpret, and make decisions together (Winarto et al, 2025). In many Iranian organizations, new technologies have either been implemented in isolation or have not been fully utilized due to employee resistance, poor digital skills, and lack of knowledge training (Rahadar et al., 2023). This has resulted in the potential capacities of digital technologies in fraud detection not being realized, and in some cases, over-reliance or complete distrust of systems has become a risk factor (Futurity Proceedings Group, 2025).

From a knowledge management perspective, accounting fraud detection requires a combination of explicit knowledge (such as rules, standards, algorithms, and reports) and tacit knowledge (such as auditor experience, professional intuition, understanding of organizational contexts, and behavioral patterns) (Han, 2023). Digital technologies are primarily capable of processing explicit and data-driven knowledge, while humans play a key role in interpretation, judgment, and final decision-making. The lack of a framework that links these two types of knowledge in the form of human-technology interaction has caused the fraud detection process to be either overly technology-driven or lacking contextual understanding, or completely human-driven and prone to errors and cognitive biases.

This theoretical and practical gap highlights the need to design a comprehensive knowledge model (Leocádio et al., 2024). In the Iranian organizational context, cultural, institutional, and structural factors also affect human-technology interaction in fraud detection. Organizational hierarchies, centralized decision-making, political and administrative considerations, fear of disclosure, and weak reporting support systems can all hinder the effective use of fraud detection technologies (Mökander et al., 2023). On the other hand, the lack of local standards and knowledge frameworks appropriate to Iranian conditions has led many organizations to simply follow foreign models; models that are not necessarily compatible with the economic, legal, and cultural realities of Iran. Therefore, designing a local model and knowledge that takes these considerations into account is a fundamental need (Desai et al., 2024).

The main issue of the present study stems from the fact that despite the expansion of digital innovations in the field of accounting and auditing in Iran, there is still no coherent, knowledge-based, and local framework for detecting accounting fraud focusing on human-technology interaction (Rashidi, 2023). Most existing studies have either focused on the technical aspects of technologies or examined the behavioral factors of fraud, without systematically linking the two. This research gap has left organizational decision-makers with no clear picture of how human knowledge and digital technology can be synergistic in fraud detection (Chen et al., 2025). On the other hand, regulatory and professional institutions in Iran, such as the Audit Organization, the Society of Certified Public Accountants, and the Central Bank, face challenges in updating fraud detection guidelines and tools in line with digital developments. The lack of a clear knowledge model has also made the process of policymaking and standards development ambiguous. In such circumstances, designing a knowledge model for accounting fraud detection can be used as a basis for strategic decision-making, human resource training, developing smart systems, and promoting financial transparency (Rezaei et al., 2024). It can be stated that the problem of the present research is the answer to this fundamental question: how can the accounting fraud detection process in Iranian organizations be improved to be more effective, intelligent, and localized by relying on digital innovations and by designing a knowledge model based on human-technology interaction? This issue is important not only from a scientific and theoretical perspective, but also from a practical perspective, it can lead to improving the financial health of organizations, increasing public trust, and strengthening economic governance in Iran. Designing such a model is a fundamental step in the transition from traditional and reactive approaches to predictive, learning, and knowledge-based approaches in the field of accounting fraud detection.

The theoretical framework of the research has been redesigned so that the detection of accounting fraud is explained not only as an accounting or auditing issue, but also as a process of processing and creating organizational knowledge based on digital innovations and human-technology interaction. In this regard, the focus of the research has shifted from describing audit tools to extracting, structuring, and integrating knowledge; in such a way that knowledge components including human knowledge of experts, technological knowledge based on data analysis and artificial intelligence, and organizational knowledge derived from organizational memory and learning, are systematically examined in the form of a knowledge model. This change of approach directly establishes the position of the article in the field of knowledge processing and knowledge-based systems.

2. Literature Review

1 -Knowledge Model of Fraud Detection

The knowledge model of fraud detection refers to a systematic framework that organizes the process of identifying, analyzing, and preventing fraud based on the production, sharing, synthesis, and application of organizational knowledge. In this model, fraud detection is not considered merely a control or monitoring activity, but rather as a learning and dynamic process that is formed from the continuous interaction between explicit knowledge (such as standards, laws, financial data, and algorithms) and tacit knowledge (such as auditors' professional experience, managerial intuition, and a contextual understanding of organizational behaviors). The main goal of this model is to improve the organization's ability to identify complex and hidden patterns of fraud through the accumulation and intelligent exploitation of knowledge (Zare Bahmaniri et al., 2023).

At the operational level, the fraud detection knowledge model emphasizes creating infrastructures for organizational learning, documenting fraud detection experiences, sharing knowledge between finance, audit, and IT departments, and continuously updating knowledge in line with environmental changes. Such a model allows organizations to move away from reactive and ad hoc approaches and towards proactive, systematic, and evidence-based approaches. In this framework, digital technologies act as facilitators of the flow of knowledge, and final decision-making remains based on informed human judgment.

2 -Accounting Fraud Detection

Accounting fraud detection refers to a set of activities, methods, and processes that aim to identify intentional distortions, misrepresentations of financial information, manipulation of accounts, and abuse of accounting procedures. This type of fraud is usually carried out with motives such as apparent improvement of financial performance, tax evasion, deceiving investors or concealing managerial inefficiencies and can seriously undermine the credibility of financial reports and the trust of stakeholders. The detection of accounting fraud is considered one of the main pillars of corporate governance and the health of the financial system. From a professional perspective, the detection of accounting fraud goes beyond formal reviews and compliance with standards and requires in-depth data analysis, identification of unusual patterns and professional judgment. As fraud tools and methods become more complex, traditional approaches based on limited sampling and manual controls have lost their effectiveness to some extent. As a result, the detection of accounting fraud today requires the use of new analytical approaches, the integration of human knowledge and advanced technologies, and attention to behavioral and organizational factors (Abdoli Abatari et al., 2024).

3 -Digital innovations

Digital innovations refer to a set of new technologies, tools, and approaches that, by relying on digital data processing, system intelligence, and network connectivity, transform traditional ways of performing organizational activities. These innovations include technologies such as artificial intelligence, machine learning, big data, blockchain, the Internet of Things, intelligent information systems, and process automation that enable fast, accurate, and predictive analysis of information. In the field of accounting and finance, these innovations play an important role in increasing transparency, accuracy, and speed of information processing (Kamrani et al., 2021; Zhang et al., 2023).

In the organizational dimension, digital innovations do not simply mean the use of technological tools, but also require changes in structures, skills, culture, and decision-making patterns. The effectiveness of these innovations depends on the organization's level of digital readiness, the ability to absorb technology, and the learning ability of human resources. In the field of accounting fraud detection, digital innovations create the most value when they are implemented within a knowledge framework and with consideration of the human role in interpretation and decision-making (Chen et al., 2025).

4 -Human-technology interaction

Human-technology interaction refers to the process of communication, collaboration, and interaction between human users and digital systems or technologies in performing organizational tasks. This concept goes beyond the simple use of technological tools and includes dimensions such as trust in the system, understanding of outputs, ability to interpret results, level of digital skill, and the role of humans in monitoring and final decision-making. In human-technology interaction, technology acts as a support for decision-making, and humans still play a central role in evaluating, judging, and controlling results. In the field of accounting fraud detection, human-technology interaction plays a decisive role in the effectiveness of intelligent systems. If users cannot understand the logic of the systems' operation or do not trust their results, the use of technology will remain superficial or symbolic. Therefore, designing appropriate interaction mechanisms, continuous training, transparency of algorithms, and strengthening users' analytical skills are the main prerequisites for achieving effective human-technology interaction and the success of fraud detection knowledge models (Mahasani et al., 2020).

The theoretical framework of this research is based on the integration of three main theoretical streams: knowledge management theory, accounting fraud detection theories, and human-technology interaction theory in the context of digital innovations. This framework attempts to show that accounting fraud detection in today's complex and digital environments is the result of the synergy of human knowledge, technological infrastructure, and effective interaction between the two; Not the result of the independent performance of each of these components From the perspective of knowledge management theory, knowledge is recognized as a strategic resource in organizations that can create sustainable competitive advantage (Nonaka & Takeuchi, 1995; Marcel et al., 2025). In the field of fraud detection, knowledge includes explicit knowledge (standards, laws, financial data, and algorithms) and tacit knowledge (auditors' experience, professional judgment, background knowledge of organizational behaviors). Nonaka's theory of organizational knowledge creation emphasizes that the effectiveness of organizations in solving complex problems depends on the continuous transformation of tacit and explicit knowledge and the dynamic flow between them. Therefore, accounting fraud detection will be effective when it is designed in the form of a knowledge and learning model.

In the following, the theoretical framework of the study relies on the literature on accounting fraud detection. The Fraud Triangle Theory proposed by Cressey considers fraud to be the result of the interaction of pressure, opportunity, and justification (Cressey, 1953). With the development of digital environments, this theory has been expanded with approaches such as the Fraud Diamond and Fraud Pentagon, which also consider factors such as individual capabilities and technological characteristics (Wolfe & Hermanson, 2004). However, most of these models have focused on behavioral or structural factors and have not integrated the role of organizational knowledge and smart technologies, a gap that the present theoretical framework seeks to fill.

In the technological dimension, the theoretical framework of the research is based on the theory of digital innovations and digital transformation. According to Brown et al., digital innovation is not limited to the application of technology, but requires a redefinition of processes, roles, and decision-making practices in the organization (Bharadwaj et al., 2013). Technologies such as artificial intelligence, machine learning, and big data analytics provide the ability to identify unusual patterns and predict fraudulent behavior, but their effectiveness depends on how they are integrated with human knowledge and organizational structures.

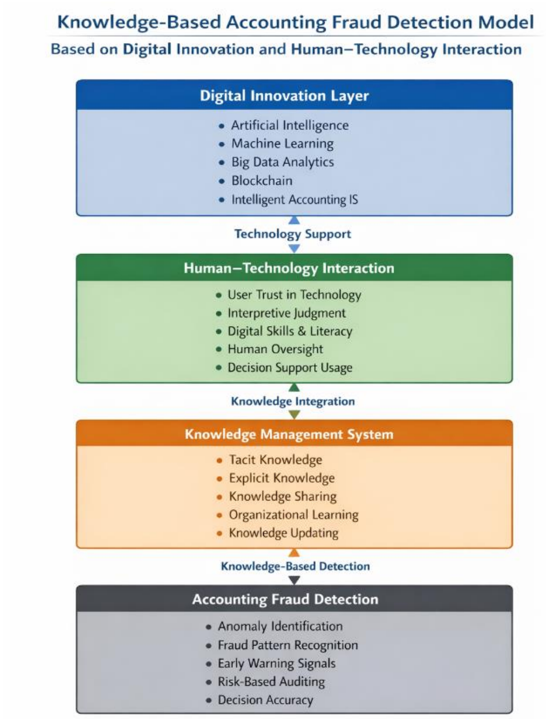


Figure 1. *Intelligent knowledge-based fraud detection model*

In this regard, the Human–Technology Interaction theory plays a central role in the theoretical framework. According to this theory, the performance of intelligent systems is maximized when human users can understand, interpret, and apply technological outputs in their decision-making (Parasuraman et al., 2000). Technology acceptance models (TAM and UTAUT) also show that variables such as trust in the system, ease of use, perceived usefulness, and digital proficiency of users play a decisive role in the effective use of technology (Venkatesh et al., 2003). In accounting fraud detection, this interaction determines whether intelligent systems become real decision-making tools or merely play a symbolic role.

Accordingly, the theoretical framework of the present study argues that digital innovations affect organizational knowledge management through human–technology interaction and ultimately lead to the improvement of accounting fraud detection. In this framework, human-technology interaction plays the role of a mediating variable that determines the intensity and direction of the impact of digital technologies on knowledge processes and fraud detection results. Also, knowledge management, as a central mechanism, integrates the knowledge produced by technology and humans and transforms it into effective control decisions. The present theoretical framework provides a systemic and knowledge-based view of accounting fraud detection that is also consistent with the conditions of Iranian organizations; because it emphasizes the role of humans, organizational learning, and technology localization and distances itself from purely technology-oriented or purely behavioral approaches. This framework can be a basis for developing a conceptual model, formulating hypotheses, and designing a native accounting fraud detection model in the context of digital transformation.

In the Designing a Knowledge Model for Accounting Fraud Detection Based on Digital Innovations with a Focus on Human–Technology Interaction in Organizations model, the relationship between knowledge and the Interpretive Structural Modeling (ISM**)** method is such that ISM functions as a systematic mechanism for structuring and explaining knowledge. Within this framework, expert knowledge from auditing and digital technology specialists serves as the primary input to ISM, and through identifying interpretive and causal relationships among human, technological, and organizational knowledge components, it is transformed into a coherent and hierarchical structure. Consequently, ISM facilitates the conversion of tacit knowledge into explicit and organizational knowledge, enables the identification of foundational and driving knowledge factors in accounting fraud detection, as well as dependent and outcome-oriented factors, and plays a pivotal role in integrating human knowledge with technological capabilities within the context of human–technology interaction.

3. Method

From a philosophical perspective, the present study is an empirical study based on a deductive-inductive approach. The aim of this study is also to present interpretive structural modeling with the aim of designing a knowledge model for detecting accounting fraud based on digital innovations with a focus on human-technology interaction in organizations. Therefore, from the perspective of the objective, it is an applied-developmental study. The interpretive structural model is one of the systematic and qualitative-analytical methods for identifying, structuring, and explaining the complex relationships between the components of a multidimensional phenomenon that is widely used, especially in management and organizational issues. This method, relying on the judgment of experts, enables the transformation of their scattered and implicit knowledge into a hierarchical and logical structure; in such a way that key variables are classified at different levels of influence and influenceability. In research related to the design of knowledge models, including the detection of accounting fraud based on digital innovations, the interpretive structural model is a suitable tool for explaining the causal relationships between human, technological, and knowledge components and helps the researcher to identify the drivers, intermediate factors, and main consequences in a coherent and interpretable manner.

Since the data in this study were collected without bias or manipulation, it is a non-experimental (descriptive) study that was conducted using a cross-sectional survey method. This research is applied in terms of its purpose and exploratory in nature, and it was conducted based on mixed methods (qualitative and quantitative). In preparing the effective components of accounting fraud detection based on digital innovations, the documentary study method and the Delphi method were used. The Delphi team was selected using a purposive sampling method of judgment. The study population of this study included accountants and financial experts. 14 people were identified as interviewees based on the purposive sampling method in the qualitative analysis. The statistical description of the characteristics of the field participants is presented in Table 1.

4. Findings

Some demographic information related to the qualitative experts is given in Table 1.

Table 1. *Some information about the interview panel members participating in the research*

Demographics	Category	Percent
Gender	Female	۵۵%
	Male	۴۵%
Experience	Under 10 years	۳۳%
	Over 11 years	۶۷%

In data processing, the structural interaction analysis method was used in MICMAC software. As a result of monitoring variables, 11 components were identified and clustered based on library studies (Table 2).

Table 2. *Component notation*

SSIM	Variable	Source
C01	Big Data Analytics	Bhattacharya(2024)
C02	Machine Learning Fraud	Han (2023)
C03	Audit Artificial Intelligence	Winarto et a (2025)
C04	Smart Transaction Tracking	Alsulami (2023)
C05	Cryptography and Transparency	Compagnino (2025)
C06	Financial Process Automation	Hernández-Aros (2024)

C07	Latent Behavioral Data Mining	Ramos (2024)
C08	Digital Anomaly Detection	Bhattacharya(2024)
C09	Financial Blockchain Platform	Han (2023)
C10	Continuous Real-Time Monitoring	Winarto et a (2025)
C11	Accounting Fraud Detection with the Approach of New Developments in the Field of Digital Technology	-

In this study, the Delphi technique was used to evaluate and fit the 11 identified components. The views of 14 experts on each indicator are shown in Table 3:

Table 3. *Evaluation and screening of indicators based on Delphi*

Questions	Average	Median	Mode	Standard deviation	Range of changes	First quartile	Second quartile	Third Quarter	Status
C01	3.302	3	3	0.599	2	3	3	4	Approved
C02	3.186	3	3	0.732	2	3	3	4	Approved
C03	3.627	4	4	0.655	2	3	4	4	Approved
C04	3.456	4	4	0.630	2	3	4	4	Approved
C05	3.255	3	3	0.658	3	3	3	4	Approved
C06	3.248	3	3	0.650	2	3	3	4	Approved
C07	3.744	4	4	0.538	2	4	4	4	Approved
C08	4	4	4	0.520	0	4	4	4	Approved
C09	3.754	4	4	0.513	2	4	4	4	Approved
C10	3.697	4	4	0.427	2	3	4	4	Approved
C11	3.767	4	4	0	1	4	4	4	Approved

The Kendall coefficient of agreement was used to calculate the consistency of expert opinions.

Table 4. *Kendall coefficient of agreement (source of research data)*

Delphie	df	Kendall coefficient	Significant value
First round	14	0.845	0.000

Based on the results of Table 4, the value of the Kendall coefficient in the first round of the Delphi technique was 0.845, which indicates that the consensus among the experts' views is high. Also, a significant value of 0.000 was obtained, which indicates that the results can be relied on with 95% confidence.

Interpretive Structural Model (ISM) design is a method for examining the effect of each variable on other variables; this design is a comprehensive approach to measuring the relationship and this design is used to develop the model framework to enable the overall objectives of the research. The data was entered into the micmac software. Table 5 shows the characteristics of the initial matrix:

Table 5. *Initial matrix specifications*

INDICATOR	VALUE
Matrix size	11
Number of iterations	2
Number of zeros	61
Number of ones	60
Number of twos	0
Number of threes	0
Number of P	0
Total	60
Fillrate	49.58678%

The interpretive structural modeling method was used to design the initial model. For this purpose, the structural self-interaction matrix (SSIM) was first formed. The relationships of the overarching constructs are indicated by four symbols: V (variable i affects j), A (variable j affects i), X (bidirectional relationship), and O (no relationship). The structural self-interaction matrix is presented in Table 6.

Table 6. *Structural self-interaction matrix of SSIM*

C11	C10	C09	C08	C07	C06	C05	C04	C03	C02	C01	SSIM
V	V	A	V	V	V	A	V	V	V		C01
V	V	A	V	X	V	A	V	X			C02
V	V	A	V	X	V	A	V				C03
V	V	A	V	A	V	A					C04
V	V	X	V	V	V						C05
V	A	A	A	A							C06
V	V	A	V								C07

V	X	A									C08
V	V										C09
V											C10
											C11

The received matrix (RM) is obtained by converting the structural self-interaction matrix into a two-valued matrix of zero and one. In the received matrix, the elements of the main diagonal are set to one. Also, to be sure, secondary relationships must be controlled. This means that if A leads to B and B leads to C, then A must lead to C. That is, if direct effects should have been included based on secondary relationships, but in practice this has not happened, the table must be corrected and the secondary relationship must also be considered. The final access matrix is presented in Table 6.

.	1 : C	2 : C	3 : C	4 : C	5 : C	6 : C	7 : C	8 : C	9 : C	10 :	11 :
1 : C1	0	4	4	6	0	19	4	14	0	14	25
2 : C2	0	2	3	4	0	14	3	10	0	10	19
3 : C3	0	3	2	4	0	14	3	10	0	10	19
4 : C4	0	0	0	0	0	2	0	1	0	1	4
5 : C5	1	10	10	14	0	33	10	26	1	26	41
6 : C6	0	0	0	0	0	0	0	0	0	0	0
7 : C7	0	3	3	4	0	14	2	10	0	10	19
8 : C8	0	0	0	0	0	1	0	0	0	1	2
9 : C9	1	10	10	14	1	33	10	26	0	26	41
10 : C10	0	0	0	0	0	1	0	1	0	0	2
11 : C11	0	0	0	0	0	0	0	0	0	0	0

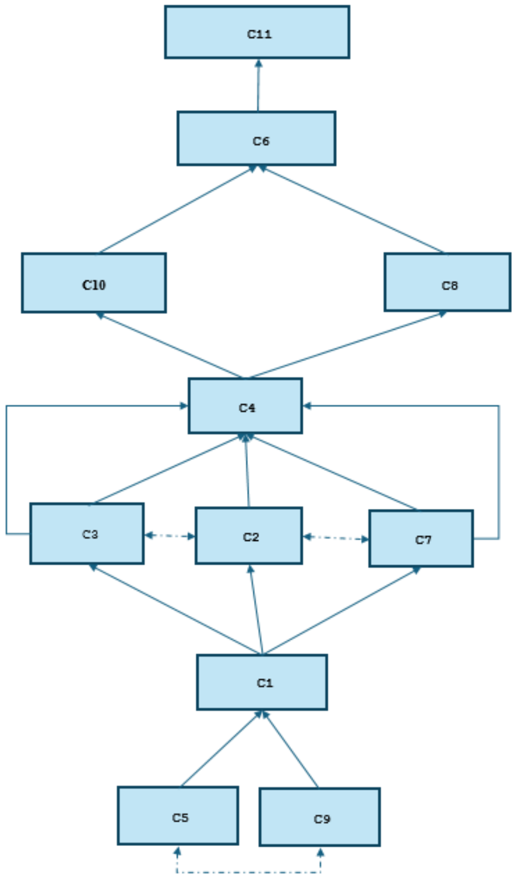
Table 7. *Final access matrix*

After forming the achievement matrix, the "achievement set" and "prerequisite set" must be identified to determine the relationships and leveling. For variable D_i, the achievement set (output or impact) includes the variables that can be reached through variable D_i. The prerequisite set (input or impact) includes the variables through which D_i can be reached. The set of inputs and outputs for determining the level is presented in Table 7.

Table 8. *Set of inputs and outputs for determining the level*

Rank	Label	Direct influence	Label	Direct dependence	Label	Indirect influence	Label	Indirect dependence
1	C5	1666	C11	1666	C5	2666	C11	2666
2	C9	1666	C6	1500	C9	2666	C6	2031
3	C1	1333	C8	1333	C1	1395	C8	1519
4	C2	1166	C10	1333	C2	1007	C10	1519
5	C3	1166	C4	1000	C3	1007	C4	713
6	C7	1166	C2	833	C7	1007	C2	496
7	C4	666	C3	833	C4	124	C3	496
8	C8	500	C7	833	C8	62	C7	496
9	C10	500	C1	333	C10	62	C1	31
10	C6	166	C5	166	C6	0	C5	15
11	C11	0	C9	166	C11	0	C9	15
Rank	Label	Potential direct influences	Label	Potential direct dependence	Label	Potential indirect influence	Label	Potential direct dependence
1	C5	1666	C11	1666	C5	2666	C11	2666
2	C9	1666	C6	1500	C9	2666	C6	2031
3	C1	1333	C8	1333	C1	1395	C8	1519
4	C2	1166	C10	1333	C2	1007	C10	1519
5	C3	1166	C4	1000	C3	1007	C4	713
6	C7	1166	C2	833	C7	1007	C2	496
7	C4	666	C3	833	C4	124	C3	496
8	C8	500	C7	833	C8	62	C7	496
9	C10	500	C1	333	C10	62	C1	31
10	C6	166	C5	166	C6	0	C5	15
11	C11	0	C9	166	C11	0	C9	15

Therefore, variable c11 is a first-level variable. After identifying the first-level variable(s), these variable(s) are removed and the set of inputs and outputs is calculated without considering the first-level variables. The common set is identified and the variables that have the same common set as the input set are selected as second-level variables. Variable C6 is a second-level variable. Variables C8-C10 are third-level variables. Variables C4 are fourth-level variables. The final pattern of levels of the identified variables is shown in the figure. In this figure, only the meaningful relationships of the elements of each level on the elements of the lower level as well as the meaningful internal relationships of the elements of each row are considered.



Evaluation of the influence and influence plan of variables

The distribution and dispersion of variables in the dispersion plane indicates the degree of stability or instability of the system. In the field of the interaction/structural analysis method with the MICMAC software, two types of dispersion have been defined in total, known as stable systems and unstable systems. In the stable system model, the dispersion of variables is in the form of L; in this model, some variables have high influence and some have high influence. However, in unstable systems, the situation is more complicated; in this system, the forces in question are dispersed around the diagonal axis of the plane and in most cases have an intermediate state of influence and influence, which makes it difficult to identify key variables. What can be understood from the state of the dispersion plane of the components is the instability state of the system. Most variables are dispersed around the diagonal axis of the plane. Except for a few cases that show that they have a high influence on the system, the rest of the variables have an almost similar state to each other (Figures 2 and 3).

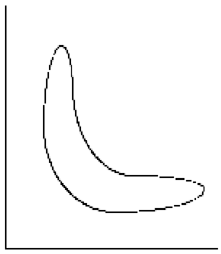
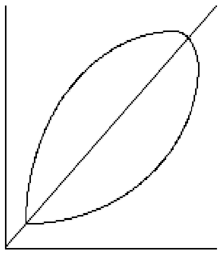



Figure 3. *Unstable system* ***Figure 2.*** *Stable system*

Figure 4 shows the dispersion pattern of the effective factors. This dispersion pattern generally indicates the state of an unstable system (Figure 4).

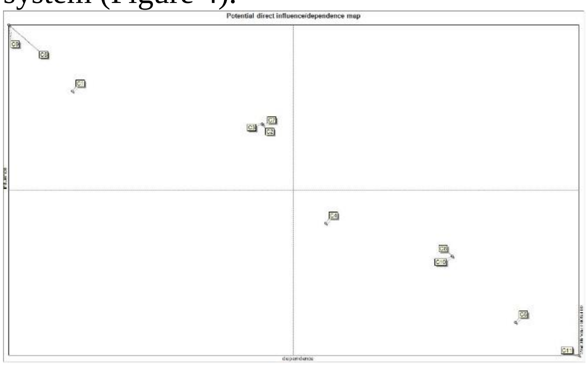


Figure 4. *Distribution pattern of influential factors*

Classification of factors affecting the model

Based on the strength of dependence and influence of variables, a coordinate system can be defined and divided into four equal parts. In this study, a group of variables were placed in the driving subgroup. These variables have high influence and low dependence. The next group is dependent variables, which are in a way the results of the product development process and are less likely to form the basis for other variables.

In this analysis, variables are divided into four groups: autonomous, dependent, linked (interface), and independent.

Autonomous: Autonomous variables have a low degree of dependence and guiding power. These criteria are generally separated from the system because they have weak connections with the system. A change in these variables does not cause serious changes in the system.

Dependent: Dependent variables have strong dependence and weak guiding power. These variables generally have high influence and little influence on the system. C11-C6-C8-C10 are dependent.

Independent: Independent variables have low dependence and high directionality, in other words, high influence and low impact are the characteristics of these variables. Based on the influence-dependence diagram, variables C5-C9-C1 have high influence and low impact and are located in the area of independent variables.

Linked: Linked or linked variables have high dependence and high directionality, in other words, the impact and impact of these criteria is very high and any small change in these variables causes fundamental changes in the system. C2-C3-C7 are linked.

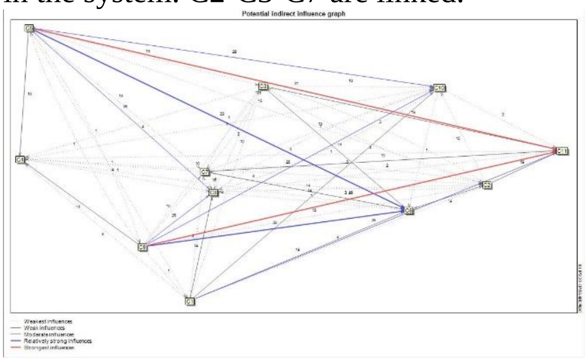


Figure 5. *Diagram of direct effects of factors (strongest effect)*

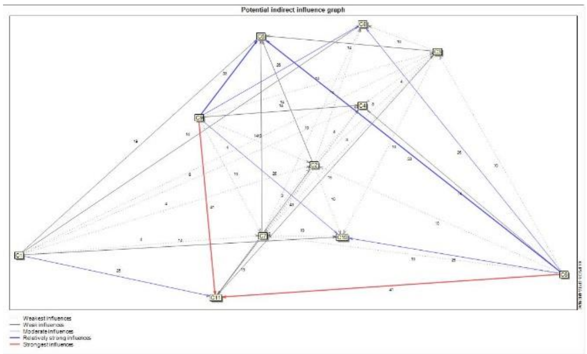


Figure 6. *Diagram of direct effects of factors (relatively strong effect)*

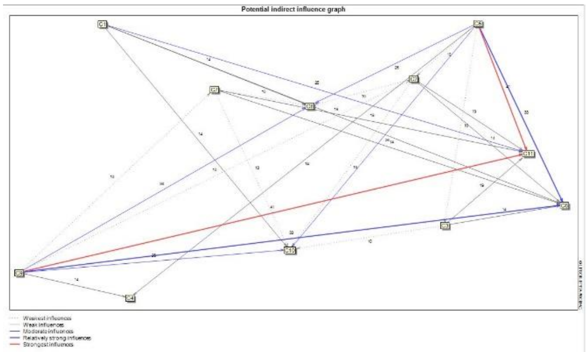


Figure 7. *Diagram of direct effects of factors (average effect)*

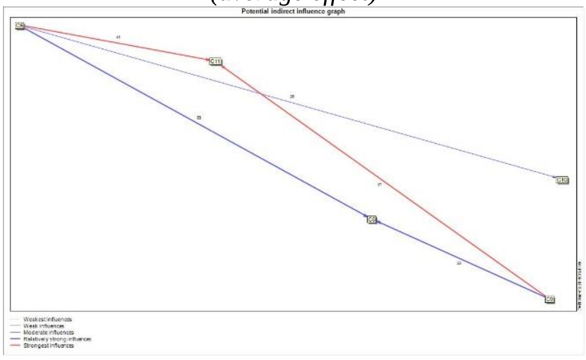


Figure 8. *Diagram of direct effects of factors (least effect)*

The proposed model is introduced as a knowledge-based system for decision-making in fraud detection that uses the interpretive structural modeling (ISM) method to engineer knowledge and extract causal relationships between knowledge components. The output of this process is the production of structured and usable knowledge to support data-driven decision-making in organizations; so that the model results can be used in the design of reasoning engines, intelligent warning systems, and decision-support dashboards based on financial data analysis. Thus, the paper goes beyond a descriptive level and establishes a clear and practical link with the fields of knowledge mining, knowledge engineering, knowledge-based systems, and data-driven decision-making.

5. Discussion

One of the key achievements of this research was the use of the method of structural interaction analysis (MICMAC), which allowed to identify dependencies and the level of influence of key variables. Based on the MICMAC analysis, the components were categorized in such a way that their underlying or influential role in the fraud detection system was determined. This categorization showed that some technologies and measures, such as big data analytics, fraud machine learning and audit artificial intelligence, act as drivers and basic factors, and the success of other components and operational layers is largely dependent on their effectiveness. This finding is consistent with previous studies in the field of financial data analytics and artificial intelligence, which show that new information technologies play a major role in improving the transparency, accuracy and speed of fraud detection (Bierstaker et al., 2006; Appelbaum et al., 2017).

Further, the analysis showed that some metrics have an intermediate or supporting role and affect more the operational and analytical layers of the system. For example, smart transaction tracking, financial process automation, and latent behavioral data mining are important at the level of the operational and analytical layers, and without the presence of basic infrastructure and smart technologies, their effectiveness will be limited. This result emphasizes the importance of designing a hierarchical and integrated structure in financial and audit organizations, so that tools and technologies at different levels operate in harmony and the flow of information and knowledge between the basic, intermediate, and operational layers is facilitated. Another achievement of the research is the identification of metrics that have a supporting and supervisory role and directly affect the control and monitoring processes. Metrics such as digital anomaly detection, financial blockchain platform, and continuous real-time monitoring were placed in higher layers of the hierarchy and act as complementary factors and enhance the effectiveness of the entire system. This finding suggests that building an intelligent fraud detection system requires simultaneous attention to both underlying technologies and monitoring and analytical tools to optimize system performance. In other words, although underlying technologies are the main drivers of the system, the full potential of the system cannot be realized without analytical and monitoring platforms. The results of the study also showed that digital transformation has caused structural changes in the financial environment that require a review of traditional audit and fraud detection methods. In addition to facilitating the analysis of large volumes of data and the identification of complex patterns, new technologies have increased the complexity of financial behavior and the relationships between components. Therefore, the use of hierarchical models and structural analysis tools such as ISM and MICMAC provides the ability to manage these complexities and prioritize key components. This finding is consistent with previous studies in the fields of risk management and information technology, which show that digital environments provide both opportunities and new challenges for fraud control (Alles, 2015; Jans et al., 2014; Qatawneh, 2024).

One of the salient aspects of this research was the identification of ten key criteria for detecting accounting fraud in the digital environment and their classification into seven hierarchical levels. This classification showed that smart technologies and data-driven tools such as big data analytics, fraud machine learning and audit artificial intelligence are at the basic level and the success of other components depends on their proper functioning. At the middle level, criteria such as intelligent transaction tracking, financial process automation and latent behavioral data mining were placed, which have an operational-analytical role. At the higher level, criteria such as digital anomaly detection, financial blockchain platform and continuous real-time monitoring were placed, which serve as monitoring and supporting factors, strengthening the functioning of the entire system.

These findings emphasize that the design and implementation of a digital technology-based fraud detection system requires a systemic and knowledge-based approach that fully considers the relationship between the basic, intermediate, and supervisory components. In other words, the success of a fraud detection system is not limited to the existence of new technologies, but rather depends on the design of an integrated knowledge framework that ensures the flow of information and knowledge between layers. This highlights the importance of human-technology interaction, human resource training, and the creation of appropriate mechanisms for data analysis and interpretation.

From an organizational perspective, the results of the study showed that the presented hierarchical model can provide a basis for managerial decision-making and internal policy-making in organizations. Understanding the drivers and underlying factors allows financial managers and auditors to allocate resources effectively, optimize control and monitoring processes, and focus on technologies and tools that are most effective in detecting and preventing fraud. Also, the leveling of components can help design training programs and develop employees' digital skills to achieve more effective human-technology interaction.

The present study also emphasizes the importance of integrating technology and human knowledge. In digital environments, intelligent systems can only be effective when human users can interpret data and system outputs and apply them in decision-making. Therefore, any fraud detection system must simultaneously include advanced technologies and knowledge mechanisms that systematically connect employees' explicit and tacit knowledge to the flow of information and decision-making. This finding is consistent with recent studies in the field of human-technology interaction and artificial intelligence, which show that the combination of human knowledge and technology is the key to maximizing the use of digital capabilities (Parasuraman et al., 2000; Venkatesh et al., 2003). From a research perspective, the results of this study can provide a framework for future research. Researchers can use the presented hierarchical model to examine the causal relationships between components in different organizations, analyze the longitudinal effects of digital innovations on fraud detection, or apply quantitative models based on SEM and network analysis to validate the presented structural relationships. In addition, this framework has the potential to be localized for Iranian organizations and developing countries, because it is designed to suit the limitations and capacities of technology, human skills, and organizational culture.

6. Conclusion

The results of this study, which aimed to develop an interpretive structural modeling of accounting fraud detection based on digital innovations, showed that digital transformation has not only provided new tools for detecting and preventing fraud, but also created more complex structures in the financial environment that require a systematic analysis of the relationships between influential factors. The application of the method of structural interaction analysis (MICMAC) made it possible to accurately assess the dependencies and influence of key variables, and finally, ten main criteria including big data analytics, fraud machine learning, audit artificial intelligence, smart transaction tracking, encryption and transparency, financial process automation, hidden behavioral data mining, digital anomaly detection, financial blockchain platform, and continuous real-time monitoring were classified into seven levels. This hierarchical classification shows that some criteria play a fundamental and fundamental role in the success of fraud detection systems, while others affect more the operational, analytical, and supervisory layers. The present study aimed to develop an interpretive structural modeling of accounting fraud detection based on digital innovations, and identified and analyzed the relationships between key components in this area. The results show that digital developments, in addition to creating new tools for detecting and preventing fraud, have created more complex structures in the financial environment, which cannot be fully exploited without systematic analysis and accurate modeling. This finding highlights the importance of adopting systematic and knowledge-based approaches to accounting fraud detection and shows that success in this area is only possible by combining new technologies and human knowledge.

It can be concluded that the present study showed that digital developments not only help create new tools, but also increase the complexities of the financial and structural environment, which cannot be fully exploited without structural modeling. The seven-level hierarchy of components identified the importance of basic technologies, intermediate metrics, and monitoring tools, and showed that effective fraud detection requires coordination across all of these layers. These findings have scientific, practical, and policy implications and can help design intelligent fraud detection systems, develop employees' digital skills, and increase the transparency and financial health of organizations. Based on the results obtained, it is suggested that:

-Organizations can strengthen their fraud detection capabilities by investing in IT infrastructure, including big data systems, artificial intelligence platforms, and machine learning. In addition to developing technological tools, it is essential to pay attention to data quality and integrity so that systems can identify fraud patterns more accurately and quickly. The use of techniques such as behavioral data mining and anomaly analysis, along with the design of coherent databases, can enable the detection of complex and hidden frauds.

-Organizations should create mechanisms that facilitate effective interaction between human users and intelligent systems. This includes continuous training of employees in data analysis and digital tools, increasing technological literacy, and creating an environment for interpreting and providing feedback on the results of intelligent systems. Strengthening users' trust in technology and the ability to interpret intelligent outputs will lead to more accurate and faster decisions and prevent superficial or symbolic use of technology.

-Organizations can record and share the flow of information and experiences related to fraud detection by setting up knowledge management systems. Combining explicit and tacit knowledge of employees with analytical data from intelligent systems allows for organizational learning and continuous improvement of fraud detection algorithms. These systems should be capable of continuous updating so that knowledge gained from real fraud cases and changes in the financial environment is quickly disseminated throughout the organization.

-Based on the findings of interpretive structural modeling, organizations should design the basic, intermediate, and supervisory components of fraud detection in a hierarchical manner to optimize the flow of information and knowledge between different levels. This design enables basic technologies such as machine learning and audit artificial intelligence to play a driving role and gives analytical and supervisory tools the necessary power to accurately detect fraud. Applying such a hierarchical framework, while reducing complexity, also allows for prioritization of actions and resource allocation.

- Implementing real-time monitoring systems and predictive algorithms allows for the rapid identification of suspicious transactions and prevention of the spread of fraud. By combining blockchain technology and data analysis tools, organizations can increase transparency and traceability of transactions and improve the level of trust of stakeholders. This approach makes fraud detection processes not only reactive, but also predictive and based on evidence and organizational knowledge.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Abdoli Abatari, Z., Mali, A., Rostami, A., & Aghaei Chadegani, A. (2023). Future of Auditing from the Perspective of Information Technology, Changing Auditor-Client Relationship and Changing the Concept of Auditing. *Professional Auditing Research*, 4(16), 66-91. [in Persian]

Alles, M. (2015). *Drivers of the use and facilitators and obstacles of the continuous auditing of financial statements*. *Accounting Horizons*, *29*(2), 439–452. https://doi.org/10.2308/acch-51063

Alsulami, R., Albalawi, R., Albalawi, M., Alsugair, H., Alblowi, K. A., & Alharbi, A. R. (2023). Review the Recent Fraud Detection Systems for Accounting Area using Blockchain Technology. *International Journal of Computer Science & Network Security*, *23*(5), 109-120.

Appelbaum, D., Kogan, A., & Vasarhelyi, M. (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-51836

Bagherian Kasgari, A., Raisi Vanani, A., Amiri, M., &Homayoun, S. (2024). Identifying financial fraud in public joint-stock companies using financial and non-financial criteria with a machine learning approach. *Smart Business Management Studies*, 13(50), 99-142. [in Persian]

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013).Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, *37*(2), 471–482.

Bhattacharya, I. (2024). Accounting fraud detection using contextual language and textual analysis. *Journal of Financial Crime*.

Bierstaker, J., Brody, R. G., & Pacini, C. (2006). Accountants' perceptions regarding fraud detection and prevention methods. *Managerial Auditing Journal*, *21*(5), 520–535. https://doi.org/10.1108/02686900610667217

Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). Deep learning in financial fraud detection: Innovations, challenges, and applications. *Data Science and Management*.

Compagnino, A. A., Maruccia, Y., Cavuoti, S., Riccio, G., Tutone, A., Crupi, R., & Pagliaro, A. (2025). An introduction to machine learning methods for fraud detection. *Applied Sciences*, *15*(21), 11787.

Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.

Desai, A., Kosse, A., & Sharples, J. (2025). Finding a needle in a haystack: a machine learning framework for anomaly detection in payment systems. *The Journal of Finance and Data Science*, *11*, 100163.

Futurity Proceedings Group. (2025). Blockchain for fraud prevention: Transforming accounting controls and audit trails. *Futurity Proceedings*.

Gkegkas, M., Kydros, D., & Pazarskis, M. (2025). Using data analytics in financial statement fraud detection and prevention: A systematic review of methods, challenges, and future directions. *Journal of Risk and Financial Management*, *18*(11), 598.

Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. *International Journal of Accounting Information Systems*, *48*, 100598.

Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: a literature review. *Humanities and Social Sciences Communications*, *11*(1), 1-22.

Jans, M., Alles, M., & Vasarhelyi, M. (2014). Continuous auditing of online financial transactions. *International Journal of Accounting Information Systems*, *15*(1), 1–27.https://doi.org/10.1016/j.accinf.2013.11.002

Kamrani, H., & Abedini, B. (2022). Developing a Fraud Detection Model for Financial Statements Using Artificial Neural Network and Support Vector Machine Methods in Companies Listed on the Tehran Bahador Stock Exchange. *Accounting and Auditing Management Knowledge*, 11(41), 285-314. [in Persian]

Khademi, S. (2024). Forensic accounting and fraud detection in the digital age, 9th International Conference on Management, Accounting, *Banking and Economics of Iran, Mashhad*. [in Persian]

Leocádio, D., & coauthors. (2024). Artificial Intelligence in auditing: A conceptual framework and systematic review. Governance (MDPI), 14(10), 238.

Mahasani, M., Nemati, Z., Najafi Soha, A., & Sarwari, F. (2021). *A Review of Fraud Detection Methods in Financial Statements: Data Mining Techniques, Diamond Theory Perspective and Forecasting Methods*, Fourth International Conference on Electrical, Computer and Mechanical Engineering, Tehran. [in Persian]

Dulgeridis, M., Schubart, C., & Dulgeridis, S. (2025). *Harnessing AI for accounting integrity: Innovations in fraud detection and prevention* (No. 4 (July 2025)). IU Discussion Papers-Business & Management.

Mijani, H., Tazarji, A. S., & Khazripour, M. R. (2025). Review of Previous Research on Blockchain Adoption in Accounting with Examination of Organizational Decision-Making Factors. *Business, Marketing, and Finance Open*, 1-11.

Mökander, J., & Floridi, L. (2023). Auditing of AI: Legal, ethical and technical approaches. *AI & Ethics*, 3, 123–142.

Nonaka, I., & Takeuchi, H. (1995).*The knowledge-creating company: How Japanese companies create the dynamics of innovation*. Oxford University Press.

Oladejo, M. T., & Jack, L. (2020). Fraud prevention and detection in a blockchain technology environment: Challenges posed to forensic accountants. *International Journal of Economics and Accounting*, 9(4), 315–335.

Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, *30*(3), 286–297. https://doi.org/10.1109/3468.844354

Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000).A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man, and Cybernetics, 30*(3), 286–297.

Qatawneh, A. M. (2025). The role of artificial intelligence in auditing and fraud detection in accounting information systems: moderating role of natural language processing. *International Journal of Organizational Analysis*, *33*(6), 1391-1409.

Rahadar, P., & Ghasemi Alvari, A. (2023). *Using big data analysis to detect patterns of fraud and financial abuse, 7th International Conference on Science and Technology of the Third Millennium of Economics, Management and Accounting of Iran*, Tehran. [in Persian]

Ramos, S., et al. (2024). Bibliometric analysis of artificial intelligence trends in auditing and fraud detection. *Contemporary Governance Review*, 8(2).

Rashidi. M. (2023). Investigating the role of audit quality in fraud detection: The perspective of clients and auditors, 9th National Conference on New Findings in Science and Technology with a Focus on Computer. *Management and Accounting*, Tehran. [in Persian]

Rezaei, N., Dianti, Z., Gholami, R., & Rahnamae Roudpeshti, F. (2023). Investigating the effect of cognitive styles on auditors' ability to detect fraud. *Financial and Auditing Research*, 2, 201-242. [in Persian]

Shevchuk, R., et al. (2025). Anomaly detection in blockchain: A systematic review of methods and applications. *Applied Sciences (MDPI)*, 15(15), 8330.

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.

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

Winarto, W. W. A. (2025). Bibliometric Analysis and Visualization: Fraud Accounting Research. *Asia Pacific Fraud Journal*, *10*(1), 107-138.

Wolfe, D. T., & Hermanson, D. R. (2004).The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, *74*(12), 38–42.

Zare Bahnemiri, M., Maleki, M., Hassankhani, F., & Ramsheh, M. (2023). Providing a framework for identifying and analyzing key drivers affecting the future of auditing in Iran with a focus on blockchain technology. *Empirical Accounting Research*, 13(3), 27-56. [in Persian]

Zhang, C., Zhu, W., Dai, J., Wu, Y. and Chen, X. (2023). Ethical impact of artificial intelligence in managerial accounting. *International Journal of Accounting Information Systems*, 49(49), p.100619.